May 9, 2022

Via Electronic Mail

Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-1090
Attn: Secretary, Securities and Exchange Commission

Re: Proposed Rules Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Requirements (File No. S7-09-22)

Ladies and Gentlemen:

The Bank Policy Institute ("BPI"), the American Bankers Association ("ABA"), the Independent Community Bankers of America ("ICBA") and the Mid-Size Bank Coalition of America ("MBCA") (collectively, the "Associations"), appreciate the opportunity to comment on the notice of proposed rulemaking (the "Proposed Rules")[1] issued by the U.S. Securities and Exchange Commission (the "Commission") for registrants regarding disclosure of material cybersecurity incidents, as well as cybersecurity risk management, strategy, and governance.[2]

---

1 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022) (to be codified at 17 C.F.R. pt. 229, 232, 239, 240, and 249).

2 BPI is a nonpartisan group representing the nation's leading banks. BPI members include universal banks, regional banks, and the major foreign banks doing business in the United States. Collectively, BPI members hold $10.7 trillion in deposits in the United States; make 68% of all loans, including trillions of dollars in funding for small businesses and household mortgages, credit cards, and auto loans; employ nearly two million Americans; and serve as a principal engine for the nation's financial innovation and economic growth. Business, Innovation, Technology and Security ("BITS"), BPI's technology policy division, provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the financial sector.

ABA is the voice of the nation's $23.3 trillion banking industry, which is composed of small, regional and large banks that together employ millions of people, safeguard $19.2

As the Commission is aware, the Proposed Rules and other new, federal notification requirements follow a series of cybersecurity attacks in the past two years that have harmed the U.S. public and private sectors.[3] With respect to financial institutions, cybersecurity threats and incidents may endanger not only individual banks and their shareholders but also consumers, as well as the stability of U.S. financial markets.[4] For this reason, the Cybersecurity and Infrastructure Security Agency ("CISA") has designated the financial services sector a "critical infrastructure" sector and "a vital component of our nation's critical infrastructure."[5] As designated by CISA, the sector includes "thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions," including our members.[6]

---

trillion in deposits and extend nearly $11 trillion in loans.

ICBA creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services. With nearly 50,000 locations nationwide, community banks constitute roughly 99% of all banks, employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding nearly $5.9 trillion in assets, over $4.9 trillion in deposits, and more than $3.5 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation, and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org.

Across the country, mid-size banks are providing financial solutions to entrepreneurs, professionals, their businesses and their families. Mid-size banks fuel their growth and build stronger connections to the communities in which they operate. MBCA is proud to be their voice and their self-help network. MBCA's member banks average less than $20 billion in size and serve customers and communities through more than 10,000 branches in all 50 states, the District of Columbia, and three U.S. territories.

3 *See*, *e.g.*, SEC, In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs, *available at* https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs (describing a cyberattack on SolarWinds Corp.).

4 *See* 87 Fed. Reg. at 16592 ("With an increase in the prevalence of cybersecurity incidents, there is an increased risk of the effect of cybersecurity incidents on the economy and registrants. Large scale cybersecurity attacks can have systemic effects on the economy as a whole, including serious effects on critical infrastructure and national security.").

5 Cybersecurity & Infrastructure Security Agency, Financial Services Sector, *available at* https://www.cisa.gov/financial-services-sector.

6 *Id*.

While cybersecurity threats are a newer challenge for companies in many industries, U.S. banks have long been a target of malicious cyber actors, and accordingly have invested in robust and ever-evolving measures to prevent, detect, and respond to cyber threats. Banks are leaders in the private sector in developing, maintaining, and enhancing cyber defenses. The industry invests billions of dollars each year in cybersecurity, shares cyber threat intelligence through a pioneering model that has been replicated across industries, and employs thousands of cybersecurity professionals in its efforts to protect not only market participants, but U.S. depositors, including the approximately 95% of U.S. households that maintain a bank account.[7]

In addition to work within the industry, banks have worked collaboratively with federal law enforcement and regulators for many years in a shared mission to prevent, detect, and respond to cyber threats and incidents. Since 2002, the Financial Services Sector Coordinating Council—a group of financial trade associations, financial utilities, and the nation's most critical financial firms—has worked collaboratively with key government agencies with the stated goal of protecting the financial services sector from cyber and physical incidents.

In recent years, as cybersecurity incident-reporting requirements have proliferated,[8] our members have also worked collaboratively with these agencies to promote harmonization of reporting requirements to achieve an appropriate balance between the benefits of incident reporting and the risks, harms, and operational burdens that may be associated with reporting, particularly during a crisis in which restoring and ensuring the security of services to customers is paramount. In this regard, the Associations welcome the creation of the Cyber Incident Reporting Council, pursuant to Congress's recent passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), which will be vested with the authority to "coordinate, deconflict, and harmonize" cyber incident reporting requirements to relieve covered entities of the burden of submitting multiple reports while working to investigate and remediate a significant incident.[9] The Associations also welcome the recent establishment of the White House Office of the National

---

7 *See* FDIC, How America Banks: Household Use of Banking and Financial Services (Dec. 17, 2021), *available at* https://www.fdic.gov/analysis/household-survey/index.html (noting that "94.6 percent of U.S. households (approximately 124.2 million) were 'banked' in 2019, meaning that at least one member of the household had a checking or savings account.").

8 *See*, *e.g.*, FDIC, Financial Institution Letter: Computer-Security Incident Notification Final Rule (Nov. 18, 2021), *available at* https://www.fdic.gov/news/financial-institution-letters/2021/fil21074.html; Strengthening American Cybersecurity Act, S. 3600, 117th Congress (2022), *available at* https://www.congress.gov/bill/117th-congress/senate-bill/3600/text?r=3&s=1#toc-H726F16E30F0545219360034278644 5B4.

9 *See* Cyber Incident Reporting for Critical Infrastructure Act, H.R. 5440, 117th Congress (2022), at § 204(b), *available at* https://www.congress.gov/bill/117th-congress/senate-bill/3600/text?r=3&s=1#toc-H726F16E30F0545219360034278644 5B4 ("The Secretary of Homeland Security, acting through the Director, shall, in consultation with the Cyber Incident Reporting Council … to the maximum extent practicable, periodically review existing regulatory requirements, including the information required in such reports, to report incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements.").

Cyber Director ("ONCD"), with the stated mission to ensure "federal coherence" in cyber policy, action, and doctrine and "improve public-private collaboration to tackle cyber challenges across sectoral lines."[10] Only a partnership and shared commitment between the public and private sectors can effectively mitigate the risk that malicious cyber actors pose to our country.

Consistent with this shared goal, since 2018, the Commission has provided guidance on public company cybersecurity disclosures ("2018 Guidance")[11] to promote clarity and consistency in reporting, while avoiding reporting requirements that could result in undue harm and security risks to market participants and others. Following the Commission's principles-based approach to disclosure requirements, the 2018 Guidance recognizes, for example, "that a company may require time to discern the implications of a cybersecurity incident," and states that the Commission does "not intend[] to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts."[12] We appreciate the statement in the preamble to the Proposed Rules that the 2018 Guidance will remain in place following the adoption of any final rules.

The Commission posits in the Proposed Rules that the 2018 Guidance is insufficient and that investors would benefit from additional detail and greater uniformity in cybersecurity reporting, but the limited materials cited lend little support for that proposition.[13] In fact, the cited materials describe the enhancements and continuing, positive trends in public companies' cybersecurity disclosures following the 2018 Guidance, and conclude that the Commission's existing disclosure regime is adequate.[14]

---

10 Office of the National Cyber Director, A Strategic Intent Statement for the Office of the National Cyber Director (Oct. 2021), *available at* https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf.

11 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018), No. 33-10459 (Feb. 21, 2018) [83 Fed. Reg. 8166 (Feb. 26, 2018)], *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf. *See* 86 Fed. Reg. at 16594 ("The guidance set forth in both the 2011 Staff Guidance and the 2018 Interpretive Release would remain in place if the Commission adopts the proposed rule amendments described in this release.").

12 2018 Guidance at 8169.

13 *See* 86 Fed. Reg. at 16607 ("[I]nvestors would benefit [from the Proposed Rules] because: (1) [m]ore informative and timely disclosure would reduce mispricing of securities in the market and facilitate their decision making; and (2) [m]ore uniform and comparable disclosures would lower search costs and information processing costs.").

14 Specifically, the Moody's survey cited by the Commission reviewed registrants' disclosures from 2018, the year the 2018 Guidance was issued, and thus provides little, if any, insight into the impact of the guidance. In fact, noting the high quality of banks' cybersecurity disclosures, Moody's expressed its view that the 2018 Guidance would, "over time, generate more consistent and reliable information" across industries. The 2020 EY review cited by the Commission found that "many companies are enhancing their cybersecurity disclosures," and noted marked increases since 2018 in disclosures on

While the Associations support aspects of the Proposed Rules, we believe change is essential in several areas, including to harmonize the Proposed Rules with the 2018 Guidance. We propose revisions in those areas.

I. Executive Summary

- While we support the policy goals of the Proposed Rules, we believe that, as currently drafted, the Proposed Rules insufficiently take into account other policy goals, including ensuring the cybersecurity of registrants; protecting the safety and soundness of financial institutions; and identifying and bringing to justice the perpetrators of serious cybercrimes.

- The Proposed Rules impose requirements for the timing and content of disclosure of material cybersecurity incidents on Form 8-K without sufficient regard for the security risks and harms that such disclosures may pose in certain circumstances. Specifically, the very fact of disclosure that a cybersecurity incident is ongoing and unremediated may adversely impact a registrant's ability to effectively respond to and remediate the incident, and significantly exacerbate the resulting risks and harms to the registrant and its shareholders, customers, and others.

    - The timing for the required disclosure of a cybersecurity incident on Form 8-K should be changed in the final rule to "four business days after the registrant has reasonably determined that the cybersecurity incident is no longer ongoing, and that public disclosure of the incident will not seriously jeopardize the security of the registrant."

    - Registrants should not be required to disclose to what extent an incident has been remediated given the security risks that such disclosure would pose to them.

    - The instructions for the Form 8-K disclosure should incorporate the Commission's statement, set forth in the preamble to the Proposed Rules, that "registrants are not expected to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity

---

board oversight of cybersecurity, and cybersecurity risks and risk management. Finally, the 2021 report of the National Associate of Corporate Directors ("NACD") specifically concluded that the Commission's current "disclosure regulations are adequate[.]". *See* Moody's Investors Service, Cyber Disclosures Reveal Varying Levels of Transparency Across High-Risk Sectors (Oct. 2, 2019), *available at* https://journalofcyberpolicy.com/ wp-content/uploads /2019/10/Moodys-Cyber-disclosures-10.19.pdf; EY, What Companies Are Disclosing About Cybersecurity Risk and Oversight in 2020 (Aug. 10, 2020), *available at* https://www.ey.com/ en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight; *See* SecurityScorecard, National Association of Corporate Directors (NACD), Cyber Threat Alliance, HIS Markit, and Diligent, The State of Cyber-Risk Disclosures of Public Companies (March 2021), *available at* https://www.nacdonline.org/insights/publications.cfm?ItemNumber=71711.

systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident."

- The final rule should allow registrants to furnish, rather than require them to file, the required Form 8-K given the short time frame for filing and difficult judgments that registrants may be required to make with respect to the scope and implications of the relevant cybersecurity incident.

- The final rule should allow for delayed disclosure of a material cybersecurity incident, for an appropriately limited period of time, (1) at the request of a United States Attorney, the Attorney General, or such individuals as may be authorized by the Attorney General, on the ground that disclosure would compromise an ongoing law enforcement investigation; (2) at the request of CISA, on the ground that disclosure would compromise an ongoing effort to disseminate threat information to, or otherwise protect, critical infrastructure; or (3) by a financial institution, at the request of the Federal Reserve, the FDIC, or the OCC, on the ground that disclosure may compromise the safety or soundness of a financial institution or the financial system.

- With respect to periodic disclosures, registrants should not be required to disclose the nature or status of remediation activities, including changes to cybersecurity policies and procedures. Such disclosure would assist threat actors seeking to identify ways to compromise the registrant's information systems, while providing little or no useful information to market participants.

- Certain definitions set forth in the Proposed Rules, including "cybersecurity incident" and "information systems," are overbroad and should be clarified in order to be workable. Specifically:

  - The definition of "cybersecurity incident" is overbroad in requiring disclosure of any incident that merely "jeopardizes" the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. This definition will pressure registrants to disclose incidents that merely have the potential to become material, notwithstanding the stated materiality threshold, including incidents that are ultimately determined to cause no actual harm or impact, resulting in inaccurate disclosures and unnecessary confusion. The word "jeopardizes" should be replaced with "results in substantial loss of" to capture incidents that are causing some actual harm, and to better harmonize the definition with the reporting standard set forth by Congress in CIRCIA.[15]

---

[15] *See* Strengthening American Cybersecurity Act, § 2242(c)(2)(i) ("A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall, at a minimum, require the occurrence of a cyber incident that leads *to substantial*

- The definition of "information systems" should be amended to exclude reference to "physical" infrastructure or otherwise clarify that it includes only physical infrastructure used for the transmission or storage of electronic data.

- The final rule should clarify the scope of incidents to be reported. Specifically, as drafted, the Proposed Rules require disclosure of "unauthorized" incidents, but the examples provided in the Proposed Rules of incidents that would need to be disclosed if material include authorized incidents with unintended consequences, such as a deliberate action by a registrant that unintentionally results in the disclosure of data.[16]

- The Commission should clarify the scope of the requirement to disclose incidents that may be considered material in the aggregate, including a list of non-exhaustive examples for reference. Unlike in the accounting and auditing contexts, registrants' information systems, network architecture, controls, policies, and procedures are dynamic, rendering comparisons between incidents difficult to make, and the nature, source, and root cause of any actual or potential cybersecurity incident may be equally difficult to assess in relation to that of prior incidents.

- The final rule should include less detailed and prescriptive requirements with respect to disclosure of registrants' cybersecurity policies and procedures, as such disclosures may pose a security risk to registrants.

- Registrants should not be required to disclose details related to a registrant's selection and oversight of third-party entities, including the mechanisms, controls, and contractual requirements leveraged to mitigate cybersecurity risks. Rather, registrants should only be required to disclose high-level information, including confirmation that policies and procedures are appropriately applied to third-party selection and ongoing oversight.

- Finally, the Associations do not support a new requirement that registrants disclose the cybersecurity expertise of members of a board of directors. The proposed requirement will have the effect of suggesting that boards without directors with such specific expertise are somehow deficient. Pressure from the SEC for public companies to designate directors with expertise in any single area may adversely impact their ability to identify and appoint directors with other experience, expertise, or capabilities they believe are appropriate for the oversight of the particular risks and opportunities the institution encounters, and may not result in more effective cyber risk oversight for the institution. Moreover, current disclosures provide investors with sufficient information as to the experience of

---

loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes[.]") (emphasis added).

16 *See* 86 Fed. Reg. at 16596.

members of the board of directors. If the Commission nonetheless believes more information is required, registrants could be required to disclose how the board of directors oversees the cybersecurity risks the company faces (*e.g.*, leveraging existing board committees).

II. Discussion of Comments on the Proposed Rules

A. Disclosure of Ongoing, Unremediated Cybersecurity Incidents Would Expose Registrants and Others to Serious Risks and Harms

The Proposed Rules would add a new Item 1.05 to Form 8-K that would require disclosure of a material cybersecurity incident within four business days after a registrant determines that it has experienced such an incident. As proposed, Item 1.05 would require disclosure of, to the extent known at the time of the filing:

(i) when the incident was discovered and whether it is ongoing;

(ii) a brief description of the nature and scope of the incident;

(iii) whether any data was stolen, altered, accessed or used for any other unauthorized purpose;

(iv) the effect of the incident on the registrant's operations; and

(v) whether the registrant has remediated or is currently remediating the incident.[17]

The Associations appreciate the Commission's request for comment about these proposed disclosure requirements, including whether the proposed disclosures could "have the unintentional effect of putting registrants at additional risk of future cybersecurity incidents," and whether specific disclosure items should be modified or eliminated.[18]

Critically, requiring registrants to disclose ongoing cybersecurity incidents, and whether the incidents have been remediated, would put registrants at risk with respect to the very incidents being disclosed. For the banking industry, such disclosure may result in harm to the safety and soundness of financial institutions, the ability of financial institutions to provide core services to consumers and businesses, financial institutions' ability to safeguard customers' funds and sensitive data, and the stability of the financial system, among other harms.

When a significant cybersecurity incident is ongoing, the very fact of disclosure will alert the threat actors present in the registrant's systems that malicious activity has been detected, causing them to engage in actions that will seriously impede the registrant's response to, and remediation of, the incident. Specifically, disclosure would be expected to cause the threat actors to speed up their efforts to cause harm, engage in techniques that obfuscate their presence

---

17 *See id.* at 16595.

18 *See id.* at 16597.

in the network, and destroy evidence of their criminal conduct. Furthermore, as a result of the disclosure, other malicious actors may seek to take advantage of the ongoing incident to cause harm to the company. In addition, if the incident that is disclosed results from a problem or vulnerability that may be present at other registrants, the disclosure can be expected to result in other malicious actors capitalizing on the information to attempt to compromise others.

By way of example, in the ransomware context, it is not uncommon for a company to identify threat actors in the network engaged in activity preparatory to encryption, including after stealing sensitive or confidential data. In that circumstance, in practice, the company proceeds to purge the threat actors as expeditiously as possible in a manner that prevents them learning that the company is taking steps to expel them. Under the Proposed Rules, however, disclosure may be required while the perpetrators are still in the company's systems. If the threat actors learn the company has identified their presence, there is a significant risk that the threat actors unleash the ransomware immediately, even if they were otherwise still engaged in preparatory activity such as expanding their access to the company's systems to maximize the reach of the ransomware. Upon disclosure of an ongoing incident, the threat actors would also be expected to take immediate steps to destroy logs and other evidence within or regarding the company's systems that enable the company to detect their whereabouts and the nature of their activities. This expected response would not only make it difficult or impossible to identify or apprehend the threat actors, but would pose security risks for the company, providing the threat actors with an opportunity to "hide" more effectively and thereby maintain a persistent presence in the network that the company is no longer in a position to detect. Thus, in this example, the disclosure of the ongoing incident may result in a ransomware attack on the registrant, an inability to identify or expel the threat actors, and the destruction of critical evidence.

Additionally, with respect to financial institutions, disclosure of a significant, ongoing cybersecurity incident may provoke unnecessary confusion among investors and depositors and market volatility as information about an ongoing cyber incident is constantly evolving. This could undercut the Commission's goal of ensuring orderly markets. Financial institutions work closely with bank regulators to manage and mitigate crisis situations to avoid such unnecessary confusion or a deposit "run" on a bank in which the public has lost confidence. The federal bank regulators recently promulgated a rule requiring banks to notify their prudential regulator confidentially within 36 hours of certain material cybersecurity incidents in part to "help reduce losses in the event a notification incident is so significant that it jeopardizes a banking organization's viability, as the [rule provides] additional time for the agencies to prepare to handle a potential failure as cost-effectively and non-disruptively as possible."[19] A requirement to publicly disclose significant, ongoing cybersecurity incidents undermines that goal, increasing the likelihood of a more disruptive, disorderly incident in which neither the bank nor its regulators can answer depositors' questions or provide sufficient reassurance that the issue is being effectively addressed. This risk would be even more pronounced to the extent a cybersecurity incident affected multiple financial institutions at the same time. In addition, a panicked or misinformed

[19] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 2299, 2304 (Jan. 12, 2021) (to be codified at C.F.R. pt. 53, 225, and 304).

reaction from consumers will divert the attention of bank leadership in the critical moments of a crisis.

Apart from whether the incident is ongoing, proposed Item 106 would require disclosure of "[w]hether the registrant has remediated or is currently remediating the incident."[20] While the Associations appreciate that the Proposed Rules would not require a registrant to "publicly disclose specific, technical information about its planned response,"[21] the mere fact of a public disclosure that an incident is or is not yet remediated increases the risk of harm to the registrant and others in connection with the incident at issue. For instance, if malicious actors are alerted to the fact that a registrant in a particular industry has been unable to remediate in a timely fashion, and is thus unable to effectively disable a particular exploit, they or other malicious actors may leverage that information to target other registrants with the same exploit. Conversely, there may be occasions where a registrant believes, in good faith, that an incident has been effectively remediated, but the malicious actor has maintained a "backdoor" into the registrant's network that it is waiting to exploit. A disclosure that an incident has been remediated may prompt the malicious actor to move quickly back into the network to capitalize on the registrant's misunderstanding before the registrant can identify that an issue has persisted.

The Associations appreciate that the Commission has acknowledged that disclosing significant, ongoing cybersecurity incidents poses a risk of harm to registrants.[22] While set forth as a "cost," the Proposed Rules do not explain why the Commission believes this cost is outweighed by the perceived benefit of public disclosure of an ongoing cybersecurity incident. Our members, including cybersecurity experts and professionals who manage their cybersecurity risk, believe the benefit is significantly outweighed by the risk of harm that disclosure would pose, as set forth above. Furthermore, these harms would not be limited to the registrant at issue and its investors, but would be faced by consumers, whose deposits and sensitive data may be at risk if the cybersecurity of banks is compromised, as well as other registrants who may be attacked by malicious actors seeking to take advantage of any broader or systemic vulnerabilities or weaknesses suggested by the disclosure.[23]

For these reasons, we believe registrants should not be required to disclose cybersecurity incidents that are ongoing, or to disclose whether an incident has been remediated. We propose that the requisite disclosure on Form 8-K be modified in the final rule to "four business

---

20 *See id.*

21 *See id.*

22 *See* 86 Fed. Reg. at 16610 ("Malicious actors could engage in further attacks based on the information [required to be disclosed], especially given that registrants would also need to make timely disclosure, which could mean that the underlying security issues might not have been completely resolved, thereby potentially exacerbating the ongoing attack. As a result, the proposed incident disclosure rules could potentially increase the vulnerability of registrants, imposing a cost on them and their investors.").

23 As noted above, such disclosure may not only result in harm to the safety and soundness of the bank, but also to customers more generally, as the bank's ability to safeguard customers' data and funds may be compromised.

days after the registrant has reasonably determined that the cybersecurity incident is no longer ongoing, and that public disclosure of the incident will not seriously jeopardize the security of the registrant." We believe this disclosure requirement appropriately balances the goals of the Proposed Rules with the goals of avoiding potential harm to registrants' security, and the safety and soundness of financial institutions.

We believe our proposal has the additional benefit of reducing the likelihood that registrants will need to correct 8-K disclosures made while a cybersecurity incident is ongoing, a significant concern based on the Proposed Rules as drafted. When an incident is ongoing, it is common for registrants' understanding of the important facts to be unclear or evolving, including as to the nature, scope, and impact of the incident, a fact essentially recognized by the 2018 Guidance but which the Proposed Rules would require registrants to disclose.[24] In requiring disclosure in this circumstance, the Proposed Rules may lead to registrants unintentionally disclosing information that is subsequently determined to be incorrect because, by definition, the nature, scope, and impact of an incident, and the extent of containment and remediation of the incident, may be changing while the attack is ongoing. At the same time, while the attack is ongoing, the registrant may not have had any meaningful opportunity to investigate and determine the accuracy of available facts.

As the Commission is aware, the mere fact of having to correct information provided in the initial Form 8-K may cause confusion and uncertainty for investors, and lead to litigation, civil liability and reputational harm for the registrant. This problem has been well-documented, resulting in criticism of registrants in follow-on litigation, for example, for failing to state facts accurately in initial public disclosures, whether the registrant's report ultimately turns out to be too negative or too positive.[25] Notably, while the Proposed Rules would provide a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Securities Exchange Act,

---

24 *See* 2018 Guidance at 8169.

25 *See*, *e.g.*, Amended Consol. Class Action Compl. ¶ 391, *In re Blackbaud, Inc. Customer Data Security Breach Litig.*, No. 3:20-mn-02972-JMC (D. S.C. Feb. 3, 2022), ECF No. 77 (allegation by class action plaintiffs that "Blackbaud failed to provide Plaintiffs and Class Members with timely and adequate notice of the extent of the Data Breach by falsely assuring them in its public statements and Notices issued prior to September 29, 2020, that the attack only impacted certain Private Information and specifically did not include SSNs" when the company's subsequent disclosures provided different information); Amended Consol. Class Action Compl. ¶ 140, *In re Equifax, Inc. Securities Litig.*, No. 1:17-cv-03463-TWT (N.D. Ga. Apr. 23, 2018), ECF No. 49 (allegation by class action plaintiffs that "[i]n the days that followed Equifax's initial disclosure of the Data Breach, new information was revealed that continue to inform the market not only of the gravity of the breach, but of the fundamental defects in the Company's data security framework that enabled the breach to occur in the first place and to go undetected for so long, and of how significant the steps to remediation would really be"); Consumer Plaintiff's First Amended Consolidated Class Action Compl. ¶ 110, *In re Target Corp. Customer Data Security Breach Litig.*, No. 0:14-md-02522-PAM (D. Minn. Dec. 1, 2014), ECF No. 258 (allegation by class action plaintiffs that "[o]n January 10, 2014, Target announced that the breach was far greater than it originally reported").

they will not provide any safe harbor for companies sued under common law theories, such as negligence, in connection with any revised disclosures that may need to be issued.

Relatedly, we request that the instructions for the Form 8-K disclosure incorporate the Commission's statement, set forth in the preamble to the Proposed Rules, that it "would not expect a registrant to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident."[26]

Finally, the Associations appreciate the Commission's request for comment as to whether registrants should be permitted to furnish rather than be required to file the required Form 8-K. We believe it is important that registrants be permitted to furnish the Form 8-K in light of the short time frame for filing, and the difficult judgments registrants may be required to make with respect to the nature, scope, and implications of the relevant cybersecurity incident. As the Commission properly acknowledges, it may take a considerable amount of time even under the best of circumstances to determine the exact nature, scope, and implications of a cybersecurity incident, and neither the registrant nor the authorized person executing the Form 8-K should have liability for disclosure judgments made in such difficult circumstances.

B. The Final Rules Should Provide a Safe Harbor for Delayed Disclosure in Limited Circumstances at the Request of Federal Bank Regulators, Federal Law Enforcement, or CISA

The Associations appreciate that the Commission has requested input on whether "any rule [should] provide that the Commission shall allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security[.]"[27] The Associations believe this potential exception should be broadened to allow delayed disclosure (1) at the request of a United States Attorney, the Attorney General, or such individuals as may be authorized by the Attorney General, on the ground that disclosure would compromise an ongoing law enforcement investigation; (2) at the request of CISA, on the ground that disclosure would compromise an ongoing effort to disseminate threat information to, or otherwise protect, critical infrastructure; or (3) by a financial institution, at the request of the Federal Reserve, the FDIC, or the OCC on the ground that disclosure may compromise the safety or soundness of a financial institution or the financial system.

An appropriately limited delay in disclosure in order not to compromise an ongoing law enforcement investigation can significantly aid registrants in responding to and remediating a cybersecurity incident. Such appropriately limited delays may enable law enforcement to gather and then share critical evidence to enable registrants to identify compromises before malicious actors can take steps to cause harm or obscure their presence. For example, law enforcement may (and often does) share known IP addresses used by the malicious actors to enable registrants to determine if any additional malicious connections to the company's network are occurring that

---

26 *See* 86 Fed. Reg. at 16595.

27 *See id.* at 16598.

would not otherwise be discernible; email addresses used by malicious actors to send spear-phishing emails, in order to enable the registrant to identify personnel, accounts, devices, or other infrastructure that are being targeted by malicious actors; and domains used by the malicious actors in order to enable the registrant to search the company's records to see if the domains were visited. If a disclosure on Form 8-K was made as proposed, however, malicious actors would be expected to take steps to hide their presence, including by using different tools and infrastructure that law enforcement and registrants will no longer be able to identify.

An appropriately limited delay in disclosure may also enable law enforcement to act quickly to identify and apprehend perpetrators of cybercrimes using evidence that the perpetrators would be expected to destroy if the incident were publicly disclosed. Given that most threat actors engage in cybercrime repeatedly (either as a part of a criminal enterprise or nation-state sponsored group), enabling law enforcement to identify and apprehend them is critical to expanding the breadth and depth of the protection afforded to registrants and market participants and to deterring others from engaging in cybercrime. This is particularly important for registrants in critical infrastructure sectors, including the financial services sector.

Separately, we believe the Proposed Rules should provide for delayed disclosure at the request of CISA in limited circumstances to support CISA's critical responsibility to "coordinate[] the execution of our national cyber defense, lead[] asset response for significant cyber incidents and ensure[] that timely and actionable information is shared across federal and non-federal and private sector partners."[28] Pursuant to the recently passed Strengthening American Cybersecurity Act of 2022, "covered entities" will be required to confidentially report a broad range of cybersecurity incidents to CISA within 72 hours[29] in part so CISA can, as appropriate, "rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures."[30] Under the Proposed Rules, however, an 8-K filing could be required within 24 hours of a required, confidential notification to CISA, undermining CISA's ability to coordinate and disseminate threat indicators and defensive measures in time for others to act on the information. Companies throughout the private sector could be harmed, since the 8-K disclosure will be useful to the threat actors (as set forth above) while being of little or no use to other companies, which may not yet have received the anonymized threat indicators and defensive measures that the Act is intended to enable CISA to provide.

---

28 Cybersecurity & Infrastructure Security Agency, About CISA, *available at* https://www.cisa.gov/about-cisa.

29 Strengthening American Cybersecurity Act, § 2242(a)(1)(A) ("A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.").

30 *See id.* at § 2245(a)(2)(A); *see also* Cybersecurity & Infrastructure Security Agency, Sharing Cyber Event Information: Observe, Act, Report Fact Sheet (April 2022), *available at* https://www.cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf ("When cyber incidents are reported quickly, CISA can use this information to render assistance and provide a warning to prevent other organizations and entities from falling victim to a similar attack.").

With respect to the bank regulators, the Federal Reserve, FDIC, and OCC are primarily responsible for overseeing and assuring the safety and soundness of the financial system, a core component of U.S. critical infrastructure. Financial institutions, including the Associations' members, work closely with these regulators to manage and mitigate potential crisis situations which may have adverse implications not only for financial institutions, but for depositors and investors, as explained above. Accordingly, we believe the final rule should provide that a financial institution may delay disclosure at the request of the federal bank regulators on the ground that disclosure may compromise the safety or soundness of the financial institution or the financial system. The final rule could limit the period or circumstances of the permissible delay as the Commission and bank regulators deem appropriate.

Against this backdrop, the Commission's proposed exception is overly narrow and unworkable both in substance and timing. Many serious cybercrimes with the potential to affect multiple registrants and other market participants are not matters of U.S. national security. And with respect to timing, even cybercrimes that implicate national security may not be identifiable as such within four days, much less also, within that time, escalated to the highest level of the Justice Department and the subject of a written nondisclosure request from the Attorney General. Separately, certain cybercrimes may be recognizable to federal bank regulators as potentially affecting the safety and soundness of a financial institution or the financial system, an area in which they have unique expertise, but may not be immediately recognizable to law enforcement as a matter of U.S. national security. Simply put, a broader exception is needed, and our proposal is intended to strike a balance between that need and the policy goals of the Proposed Rules.

The lack of an exception in the Proposed Rules is also inconsistent with existing laws across the United States, at the federal and state levels, that authorize delayed disclosure at the request of law enforcement to avoid compromising an ongoing investigation. As reporting requirements have proliferated, legislators and regulators have uniformly provided either that reporting on cyber incidents will be protected from public disclosure (as in the Strengthening American Cybersecurity Act of 2022) or they have included safe harbors that authorize delayed disclosure to the public at the request of law enforcement. All 50 states have passed laws authorizing delayed disclosure to consumers of breaches of their sensitive personal data at the request of law enforcement to avoid compromising an ongoing investigation; the Gramm-Leach-Bliley Act similarly authorizes such delayed disclosure by financial institutions;[31] and federal law enforcement agencies make such requests of registrants in appropriate circumstances.[32] Without

---

31 *See* 12 C.F.R. App. B to Part 30(III)(A) ("Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.").

32 *Cf*. 45 C.F.R. § 164.412 ("If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification,

a corresponding law enforcement exception, the Proposed Rules would undermine the determination of all U.S. states and numerous federal agencies that law enforcement's need to protect the public weighs in favor of a disclosure delay in limited circumstances. In that respect, the Proposed Rules would also be in conflict with the mission of the ONCD.[33] Thus, while the Proposed Rules serve an important purpose, we believe a limited safe harbor is critical to the protection of registrants, market participants, and our shared commitment to enhancing the nation's ability to prevent, detect, and respond to cybercrime, as well as to the government's stated mission of ensuring coherence and promoting the public-private partnership in cybersecurity.[34]

C. The Final Rules Should Not Require Registrants to Disclose the Nature of Remedial Efforts

Proposed new Item 106 of Regulation S-K would require updated disclosure in Quarterly Reports on Form 10-Q and Annual Reports on Form 10-K of material changes, additions, or updates to previously disclosed cybersecurity incidents including, in relevant part, "[a]ny changes in the registrant's policies and procedures resulting from the cybersecurity incident, and how the incident may have informed such changes."[35]

---

notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.").

33 White House, Office of the National Cyber Director, *available at* https://www.whitehouse.gov/oncd/ (describing its mission of "ensuring federal coherence" and "improving public-private collaboration" in cybersecurity).

34 *See*, *e.g.*, Exec. Order No. 14028, § 1 (May 12, 2021), *available at* https://public-inspection.federalregister.gov/2021-10460.pdf ("But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector."); Office of the National Cyber Director, A Strategic Intent Statement for the Office of the National Cyber Director (Oct. 2021), *available at* https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf ("Taken together, and in partnership with the National Security Council, the Office of Management and Budget, fellow White House offices, the Cybersecurity and Infrastructure Security Agency and its partner Sector Risk Management Agencies, government stakeholders at every level, and, of course, the private sector, these efforts will improve our ability to collaborate, take Americans off the front lines of cyber conflict, and improve our national and economic security.").

35 *See* 86 Fed. Reg. at 16598 (listing non-exclusive examples of the type of disclosure that should be provided, if applicable, including: (i) any material impact of the incident on the registrant's operations and financial condition; (ii) any potential material future impacts on the registrant's operations and financial condition; (iii) whether the registrant has remediated or is currently remediating the incident; and (iv) any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes).

Financial institutions employ multi-layered and changing defenses to ensure their cybersecurity. Their policies and procedures in this regard are highly sensitive and confidential, and are closely held even within the organization because disclosure of them or any part of them may jeopardize the company's security. Requiring registrants to disclose changes in their cybersecurity policies and defense procedures would assist malicious actors looking for ways to compromise them, while providing virtually no benefit to investors, who are ill-equipped to assess the nature and significance of the changes, particularly without an understanding of the registrant's unique and complex information systems, infrastructure, and technology.

The Associations appreciate the Commission's recognition that the detailed disclosures required by the Proposed Rules on this sensitive subject may increase the risk of future cyberattacks on registrants.[36] The Associations do not agree, however, that the concern should be discounted due to the fact that "academic research so far has not provided evidence that more detailed cybersecurity risk disclosures would necessarily lead to more attacks."[37] The limited studies cited by the Commission did not assess the impact of disclosing the nature and status of remedial efforts to address cybersecurity incidents, including changes to policies and procedures, which we believe registrants generally do not provide given the sensitivity of the information. Nor did the studies consider the views of information security professionals, law enforcement, or other experts on the impact such disclosures would be expected to have on registrants and others. And while the Proposed Rules focus on the potential that these disclosures may increase the risk of future cyberattacks, they fail to acknowledge the detrimental impact such disclosure may have with respect to the very incident the registrant is working to remediate. A registrant disclosing to the public that it has not yet been able to remediate a material incident, and thus remains vulnerable in a particular regard, may enable cybercriminals to target and frustrate the registrant's remedial efforts.

The Commission also suggests that these disclosures will enable investors to determine "which [registrants] have weak policies and procedures related to cybersecurity risk management,"[38] but the nature and status of remediation may (and frequently does) reflect not the quality of the remediation or preexisting policies and procedures, but the nature of the relevant incident and the company's information systems, infrastructure, and technology. For example, certain incidents may take weeks or months to remediate, not because the registrant has inadequate procedures or insufficiently prioritizes cybersecurity, but because the remediation requires complex measures that affect interrelated systems and procedures and cannot proceed more quickly without introducing even greater risks or harms. Similarly, particular changes, or a lack of changes, to policies and procedures following an incident may not correlate with the quality of the registrant's cyber risk management, and as noted above, the very disclosure of these changes may impair that function.

---

36 *See*, *e.g.*, *id*. at 16610 ("The concern is that malicious actors could use the disclosures to potentially gain insights into a registrant's practices on cybersecurity issues and thus better calibrate future attacks.").

37 *See id.* at 16610.

38 *See id.*

The Commission further suggests that the detailed disclosures required by the Proposed Rules will benefit critical infrastructure providers by ensuring that threat information is promptly disseminated to them. In fact, CISA already has responsibility for collecting and disseminating such information, and it does so in a confidential manner, with detailed and actionable information that is critical to registrants' ability to take preventative and responsive measures. Members of critical infrastructure industries also already routinely share detailed and actionable threat intelligence with each other. For example, the Associations include founding members of the Financial Services Information Sharing and Analysis Center, the global, cyber-threat intelligence-sharing community focused on the financial services sector that has become a model for cyber information-sharing for industries worldwide. As with the information shared by CISA, what is crucial for registrants in these information-sharing channels is the dissemination of specific, technical, and confidential information that they can act upon, none of which the disclosures under the Proposed Rules would provide.

Similarly, the Commission suggests that the Proposed Rules may benefit consumers, who can use the disclosures to decide how well a registrant protects their sensitive personal information. In fact, premature disclosure of a cybersecurity incident will result in confusion and frustration among consumers whose essential questions—whether and to what extent their own personal information was impacted—are often unanswerable so soon after the incident is discovered. For this reason, data breach disclosure laws in every state provide companies with a reasonable amount of time, which varies by state, in which to identify and notify impacted individuals. By contrast, disclosures under the Proposed Rules may result in a deluge of incoming questions from consumers that cannot be answered, which is unhelpful and even harmful to consumers, would cause reputational harm to the registrant, and will divert management's attention from the crucial task of recovery from a significant incident.

Finally, the Proposed Rules would require quarterly or annual disclosure of "any material changes, additions, or updates to the information required to be disclosed pursuant to Item 1.05 of Form 8-K."[39] The Associations' understanding of this proposed requirement is that after a cybersecurity incident ceases to be material, such updated disclosures will no longer be required.

D. The Definitions of "Cybersecurity Incident" and "Information Systems" Require Clarification

The Proposed Rules would require current and periodic reporting of material "cybersecurity incidents."[40] A "cybersecurity incident" would be defined as "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."[41] The Proposed Rules further define "information systems" as "information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing,

---

39 *See id.* at 16598.

40 *See id.* at 16595.

41 *See id.* at 16601.

maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations."[42]

The Associations appreciate that the Commission sought generally to align the Proposed Rules' definitions with existing definitions.[43] The Associations also appreciate that the Commission has requested comment as to whether these definitions should be modified, including whether registrants would "be reasonably able to obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them."[44] The Associations believe certain revisions to the proposed definitions are necessary.

First, as currently drafted, the definition of "cybersecurity incident" is overbroad in that it includes any unauthorized occurrence on or conducted through a registrant's information systems that *jeopardizes* the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. Cyber incidents of all kinds may "jeopardize" a portion of a system or some information within it, but in practice, soon be determined to not to cause any harm. But a disclosure requirement that forces registrants to disclose all incidents that could have significant effect—essentially, a requirement to predict at the outset of an incident whether the incident will cause significant harm—will result in disclosure of incidents as "material" (because they involve some risk of such harm) that are soon determined to be immaterial (because they do not involve any such harm). In other words, by including the concept of "jeopardy," or potential harm, the definition will result in over-disclosure of incidents or potential incidents that are subsequently determined not to be harmful, much less materially harmful. These inadvertently inaccurate disclosures may result in mispricing of the company's securities, lawsuits, and reputational harm. To avoid this result, the final rule should replace "jeopardizes" with "results in substantial loss of," a phrase that also better aligns with the definition set forth by Congress in CIRCIA.[45]

Separately, by including physical infrastructure in the proposed definition of "information systems" (*i.e.*, "physical . . . infrastructure . . . for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information"), the definition may be read to capture infrastructure storing physical documents and records, and thus to result in a definition of "cybersecurity incident" that includes the destruction of physical documents and records. We do not believe this is the Commission's intent, and would propose either deleting the word "physical" or clarifying that the Commission is referring only to physical infrastructure for the processing or storage of electronic data.

Regarding the proposed definition of "information systems" that includes systems that are merely used, but not owned, by the registrant, it is important to emphasize that registrants are typically limited in their ability to obtain information from service providers that would enable

---

42 *See id.*

43 *See id.* at 16595, 16600-16601, n.80.

44 *See id.* at 16598; *see also id.* at 16601.

45 *See* Strengthening American Cybersecurity Act, § 2242(c)(2).

registrants to make a materiality determination. Certain service providers are required to provide certain breach information to registrants either by regulation or contract, but there is no uniform requirement that applies to service providers. As such, while registrants can make materiality determinations with the information they have, they do not have a unilateral ability to obtain relevant information in all circumstances, particularly with respect to information that resides with third parties. The final rule should reflect this reality, by way of a safe harbor or otherwise.

Finally, the Associations request clarification as to the scope of cybersecurity incidents that would need to be disclosed. While the Proposed Rules refer to "unauthorized" incidents, they include as an example of an incident that would require disclosure, if material, a situation involving the accidental disclosure of data in connection with an action undertaken by the registrant. In the cybersecurity context, deliberate actions are not typically considered "unauthorized," even if they result in unintended consequences. It is unclear whether the Commission intends the rule to capture malicious incidents, as drafted, or even more broadly to include unintentional incidents, such as those caused by outages or technology or other errors.

E. The Requirement to Disclose Cybersecurity Incidents that Have Become Material in the Aggregate Requires Clarification

The Proposed Rules would also require registrants to disclose, to the extent known to management, when a series of previously undisclosed cybersecurity incidents that were individually immaterial have become material when viewed in the aggregate. The Associations request clarification of the meaning and scope of this requirement, including by reference to a list of non-exhaustive examples.

The Associations appreciate that the Commission provided one example of when certain incidents may be considered material in the aggregate,[46] but in practice, this requirement may be operationally challenging and overly burdensome to attempt to comply with. For instance, it is unclear how far back in time, what type of information, and in what level of depth registrants would be expected to undertake such a review. In addition, registrants' information systems, architecture, policies, and procedures are dynamic, as are the risks they face, which would make it extremely challenging to assess what and how to aggregate, and to compare incidents and the root causes of those incidents. In this regard, cybersecurity is very different from, for example, financial accounting and auditing, which are susceptible to much better defined and uniform standards that relatively rarely change.

Finally, the Associations appreciate the Commission's invitation to comment on whether registrants should have to provide disclosure on Form 10-Q, 10-K, or 8-K "when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material

---

[46] *See id.* at 16599 (noting that "while such incidents conceptually could take a variety of forms, an example would be where one malicious actor engages in a number of smaller but continuous cyber-attacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material, or both.").

in the aggregate[.]"[47] The Associations believe that, if required, such disclosure should be provided on Form 10-K.

F. Disclosures Concerning Cybersecurity Policies and Procedures Are Unduly Prescriptive

The Proposed Rules would require registrants to disclose in their Form 10-K policies and procedures for identifying and managing cybersecurity risks, including as to operational risk, intellectual property theft, fraud, extortion, harm to employees or customers, violation of privacy laws and other litigation and legal risks, and reputational risks.[48] Those proposed disclosures would also include a description of the cybersecurity risk assessment program, including whether it engages assessors, consultants, auditors, or other third parties in connection with its cybersecurity risk assessment program, whether it has policies and procedures used to oversee and identify cybersecurity risks associated with third-party service providers (as well as contractual and other mechanisms used to mitigate cybersecurity risks with those providers), whether it undertakes activities to prevent, detect, and minimize the effects of cybersecurity incidents, and whether the company has business continuity, contingency, and recovery plans in the event of a cybersecurity incident.[49] The Associations are concerned that these contemplated disclosures are too detailed.

These detailed disclosures called for by the Proposed Rules are problematic for a number of reasons: they place outsized emphasis on one risk facing companies; by prescribing the particular points of cybersecurity policies and procedures, the Commission is effectively signaling *how* registrants should be managing cybersecurity risks;[50] and they would provide information that is less meaningful to investors but may expose the registrant to security risk by disclosing to malicious actors how the registrant manages its cybersecurity risk. The Associations believe these details are not necessary, and that existing rules regarding disclosure of risk management in connection with Management's Discussion and Analysis should suffice. If the Commission does not view existing rules as sufficient, then disclosures in connection with Management's Discussion and Analysis could be supplemented to include a principles-based discussion of cybersecurity risk management and strategy.

---

47 *See id.*

48 *See id.* at 16600.

49 *See id*.

50 *See* SEC, Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal (March 9, 2022), *available at* https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922 ("Again, while cloaked as a disclosure requirement, the proposed rules pressure companies to consider adapting their existing policies and procedures to conform to the Commission's preferred approach, embodied in eight specific disclosure items. The enumerated disclosure topics likely make sense for many public companies, but securities regulators are not best suited to design cybersecurity programs to be effective for all companies, in all industries, across time.").

G. Disclosure Concerning Cybersecurity Considerations With Respect to Third-Party Service Providers Should Be Limited to Avoid Exposing Registrants to Security Risks

Under the Proposed Rules, registrants would be required to disclose whether and how cybersecurity concerns affect a registrant's selection and oversight of third-party entities.[51] The Associations believe that disclosure of whether and how cybersecurity considerations affect registrants' selection and oversight of third parties should only be provided at a high level, as detailed information may provide a roadmap for malicious actors of vulnerabilities or weaknesses at a registrant or on a more widespread basis among companies. Specifically, 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, and registrants should not be required to include detail as to the mechanisms, controls, and contractual requirements leveraged to mitigate cybersecurity risks related to third-party providers.

H. Registrants Should Not Be Required to Disclose and Characterize the Cybersecurity Expertise of Members of the Board of Directors

Proposed Item 407(j) would require registrants to disclose, in proxy statements and Annual Reports on Form 10-K, whether any member of the board of directors has cybersecurity expertise and, if so, the director's name and details sufficient to fully describe the nature of the expertise.[52] Proposed Item 407(j) would not define "cybersecurity expertise," but would include the following non-exclusive list of criteria to be considered in determining whether a director has expertise in cybersecurity: "Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner; [w]hether the director has obtained a certification or degree in cybersecurity; and [w]hether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning."[53]

While the Associations agree that cybersecurity is a significant risk that requires appropriate board oversight, we believe the proposed disclosure requirement is problematic. The proposed requirement will have the effect of suggesting that boards without directors with such specific expertise are somehow deficient, and it comes in the context of other proposed requirements that have the overall effect of encouraging companies to supplant directors with expertise overseeing diverse risks and complex institutions with those who have single subject-matter expertise akin to that of senior managers.[54] As the Commission is aware, however, the

---

51 *See id.* at 16607.

52 *See id.* at 16601.

53 *See id.* at 16602.

54 *See also* The Enhancement and Standardization of Climate-Related Disclosures for Investors, 87 Fed. Reg. 21334 (Apr. 11, 2020) (to be codified at 17 C.F.R. pt. 210, 229,

board serves an oversight role, and it is not intended to duplicate or supplant management role's to provide subject matter expertise required to manage day-to-day operations to achieve the registrant's goals.

Boards are, by design, deliberative bodies tasked with oversight of numerous, complex, and inter-related risks, of which cybersecurity is one.[55] To the extent boards, in their discretion, believe they would benefit from additional expertise and insight, they have long found ways to obtain it, including by consulting with independent experts.[56] We believe that a board composed of "special interest" directors is not the best way to advance the collective oversight of these or any other risks, and that registrants are best equipped to identify board members with the collective experience, knowledge, and judgment to oversee the particular risks they face and select and retain competent management.

232, 239, and 240) (noting, at 21359, that the "proposed item would require disclosure of whether any member of a registrant's board of directors has expertise in climate-related risks[.]").

55 *See generally* Board of Governors of the Federal Reserve System, SR Letter 21-3 / CA 21-1: Supervisory Guidance on Board of Directors' Effectiveness (Feb. 26, 2021), *available at* https://www.federalreserve.gov/supervisionreg/srletters/SR2103.htm (describing five key attributes of effective boards).

56 *See* Gregg Rozansky, Bank Policy Institute, 2021 Exposure Draft, Guiding Principles for Enhancing U.S. Banking Organization Corporate Governance (Jan. 12, 2021), *available at* https://bpi.com/guiding-principles-for-enhancing-u-s-banking-organization-corporate-governance/ (for a discussion regarding board composition and the merits of having a board with a diversity of experiences and perspectives to draw upon).

An assessment of the collective capabilities of the board and how the board works together is more meaningful than an assessment of individual skills. Accordingly, boards themselves should make their own determinations on how best to ensure an appropriately knowledgeable perspective on technology-related matters for purposes of carrying out their oversight responsibilities—*i.e.*, whether for (i) one or more board member(s) to have particular expertise, (ii) the board to retain external experts for briefings or guidance or education (*e.g.*, for board members to be brought up-to-date on key developments and, more generally, maintain an appropriately knowledgeable perspective and awareness on technology-related issues), and/or (iii) the board to rely on their access to the financial institution's own resources or staff with such expertise, as well as assessments by third parties engaged by management. *See* OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations and Insured Federal Branches; Integration of Regulations, 79 Fed. Reg. 54517 (Sept. 11, 2014) (codified at 12 C.F.R. pt. 30, 168, 170) (clarifying that the board of directors of a large national bank may rely on risk assessments and reports prepared by independent risk management and internal audit to meet its responsibilities to provide active oversight).

Pressuring registrants to designate directors with expertise in any single area may adversely impact their ability to identify and appoint directors with other attributes they believe are appropriate for the oversight of other risks their particular institution may face. Technical "experts" may not have other critical experience or capabilities complementing skill needs for the board on a collective basis. As the Commission is undoubtedly aware, there are a limited number of cybersecurity experts, and an even more limited number of such experts with experience in other areas critical to the oversight of public companies. Registrants should have the flexibility to choose whether to appoint single subject-matter experts to fill the limited seats on a board, particularly at boards of heavily regulated and complex institutions like the Associations' members, which must oversee a range of complex, diverse, and potentially inter-related risks. Some registrants may find that an approach of having a single subject-matter expert results in less effective oversight overall as one individual naturally assumes outsize responsibility and authority with respect to a critical risk that is the responsibility of the collective board to oversee.

The proposed requirement is separately problematic because it is not clear that the types of expertise given as examples in the Proposed Rules, including having a cybersecurity certification, are necessary or sufficient for oversight of cybersecurity risk at a complex organization. Moreover, registrants' current, required disclosures provide investors with ample information as to the experience of members of the board of directors, so there is no risk that investors are not informed of board members' relevant experience.[57] If the Commission nonetheless feels that more information is needed, registrants could be required to disclose how the board of directors oversees the cybersecurity risks the company faces. While we do not believe such a requirement is needed, we believe it would more be useful to investors than the disclosure required by the Proposed Rules and would avoid the potential harms we have identified with the proposed disclosure.

* * *

The Associations appreciate the opportunity to comment on the notice of proposed rulemaking. The Associations appreciate the Commission's mission to protect the investors, and we believe our recommendations will not diminish that protection, while better protecting the investor community as a whole and the national interest. The Associations intend to continue jointly discussing the Proposed Rules, and look forward to opportunities to engage in discussion

---

[57] *See*, *e.g.*, Proxy Disclosure Enhancements, 74 Fed. Reg. 68333 (Dec. 23, 2009) (codified at 17 C.F.R. pt. 274) ("For each director, briefly discuss the specific experience, qualifications, attributes, or skills that led to the conclusion that the person should serve as a director for the Registrant at the time that the disclosure is made, in light of the Registrant's business and structure. If material, this disclosure should cover more than the past five years, including information about the person's particular areas of expertise or other relevant qualifications."). In connection with this rule, the Commission stated that "companies and other proponents should be afforded flexibility in determining the information about a director's or nominee's skills, qualifications or particular area of expertise that would benefit the company and should be disclosed to shareholders." *Id*. at 68343.

with the Commission in the post-comment period on the areas of the Proposed Rules that require further clarity.

If you have any questions or would like to discuss these comments further, please reach out to Christopher Feeney at (202) 289-4322 (chris.feeney@bpi.com), Paul Benda at (202) 663-5256 (*pbenda@aba.com*), Christopher Cole at (202) 425-6533 (*chris.cole@icba.org*), or Brent Tjarks (213) 335-4344 (*brent.tjarks@midsizebanks.com*).

Respectfully submitted,

Christopher Feeney
EVP and President, BITS
Bank Policy Institute

Paul Benda
Senior Vice President, Operational Risk and Cybersecurity
American Bankers Association

Christopher Cole
Executive Vice President& Senior Regulatory Counsel
Independent Community Bankers of America

Brent Tjarks
Executive Director
The Mid-Size Bank Coalition of America