May 22, 2025

Via Electronic Mail

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Re: Petition for Rulemaking on the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule

Dear Ms. Countryman,

The American Bankers Association,[1] Bank Policy Institute,[2] Securities Industry and Financial Markets Association,[3] Independent Community Bankers of America,[4] and Institute of International Bankers[5] respectfully petition the Securities and Exchange Commission pursuant to Rule 192 of the SEC's

[1] The American Bankers Association is the voice of the nation's $24.1 trillion banking industry, which is composed of small, regional, and large banks that together employ approximately 2.1 million people, safeguard $19.2 trillion in deposits, and extend $12.7 trillion in loans.

[2] The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. The Institute produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues. 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.

[3] 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").

[4] The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams.

[5] The Institute of International Bankers ("IIB") represents the U.S. operations of internationally headquartered financial institutions from more than 35 countries around the world. The membership consists principally of international banks that operate branches, agencies, bank subsidiaries, and broker-dealer subsidiaries in the United States. The IIB works to ensure a level playing field for these institutions, which are an important source of

Rules of Practice,[6] for a rulemaking to amend the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule. When the rule was first proposed and enacted, concerns that the SEC had exceeded its authority and expertise and that the rule was deeply flawed were raised by the dissenting commissioners, by Congress, and by businesses across multiple sectors, including the financial services industry.[7] While we continue to have significant concerns regarding the rule as a whole—including the requirements of Regulation S-K Item 106 relating to cybersecurity risk management, strategy, and governance disclosures—we believe the most urgent and problematic aspects are the cybersecurity incident disclosure mandates under Form 8-K Item 1.05 for domestic issuers and under Form 6-K for foreign private issuers, both of which require rapid—often premature— disclosure of material cybersecurity incidents. These requirements impose additional risks, cost, and complexity on SEC registrants, undermining the SEC's mission to facilitate capital formation, while also failing to generate the type of decision-useful information which would advance the SEC's mission to protect investors. Accordingly, this petition requests the rescission of both Form 8-K Item 1.05 and the corresponding Form 6-K requirements.[8]

In the year and a half since Item 1.05 became effective, the fears expressed by industry have manifested.

- **Premature Disclosure**: Registrants have been forced to publicly disclose an incident even if it is ongoing, the company's investigation is not complete, and the incident has not been fully remediated.
- **Unhelpful to Investors**: The premature disclosure has harmed registrants and at the same time failed to provide the market with meaningful or actionable information upon which to make investment decisions.
- **Confusion**: The rule has been met with significant confusion, including about when to file under Item 1.05, 8.01 or neither. This has persisted despite the SEC's repeated attempts to clarify the rule through Compliance & Disclosure Interpretations,[9] commissioner statements,[10] and comment letters.[11]

---

credit for U.S. borrowers and comprise the majority of U.S. primary dealers. These institutions also enhance the depth and liquidity of U.S. financial markets and contribute significantly to the U.S. economy through direct employment of U.S. citizens, as well as through other operating and capital expenditures.

[6] 17 C.F.R. § 201.192(a).

[7] *See* Bank Policy Institute, American Bankers Assoc., Independent Community Bankers of America, and Mid-Size Banking Coalition of America, Comment Letter on Proposed Rules Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Requirements (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128336-291093.pdf [hereinafter BPI Comment Letter].

[8] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51945 (Aug. 4, 2023) [hereinafter Cybersecurity Disclosure Rule].

[9] *Compliance and Disclosure Interpretations*, Exchange Act Form 8-K, Questions 104B.01 – 104B.09 (June 24, 2024), U.S. SEC. & EXCH. COMM'N., https://www.sec.gov/rules-regulations/staff-guidance/compliance-disclosure-interpretations/exchange-act-form-8-k#104b.

[10] Erik Gerding, *Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents*, U.S. SEC. & EXCH. COMM'N. (May 21, 2024), https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024 [hereinafter Gerding Statement].

[11] The SEC issued comment letters to most of the registrants that filed Item 1.05 Forms 8-K in the first seven months the rule was in effect, and many of those letters demonstrate a fundamental disagreement between registrants and the SEC in the interpretation of the rule. *See, e.g.*, Letter from the Staff of the Div. of Corp. Fin., Sec. & Exch. Comm'n, to AT&T Inc. (July 26, 2024), https://www.sec.gov/Archives/edgar/data/732717/000000000024008480/filename1.pdf; Letter from the Staff of the Div. of Corp. Fin., Sec. & Exch. Comm'n, to AT&T Inc. (Aug. 19, 2024),

- **Weaponization by Hackers**: In multiple instances threat actors have used the rule's prescriptive requirements as additional extortion leverage.[12]

The SEC previously expressed that it was not persuaded that the risks relating to Item 1.05 identified by industry would come to pass. The staff of the SEC has since found it necessary to create a patchwork of guidance and comment letters in an attempt to address these risks. We continue to believe that Item 1.05 was flawed in its conception, and request that the SEC review the record and reconsider.

We respectfully request that the SEC rescind Item 1.05 because: (1) publicly disclosing cybersecurity incidents directly conflicts with confidential reporting requirements intended to protect critical infrastructure and warn potential victims, thereby compromising coordinated regulatory efforts to enhance national cybersecurity; (2) the complex and narrow disclosure delay mechanism interferes with incident response and law enforcement investigations; (3) it has created market confusion and uncertainty as companies struggle to distinguish between mandatory and voluntary disclosures; (4) the incident disclosure requirement has been weaponized as an extortion method by ransomware criminals to further malicious objectives, and may subject disclosing companies to additional cybersecurity threats; (5) insurance and liability implications of premature disclosures can exacerbate financial and operational harm to registrants; and (6) the public disclosure requirement risks chilling candid internal communications and routine information sharing.

Critically, without Item 1.05, investor interests will still be protected, and we believe they would be better served, through the pre-existing disclosure framework for reporting material information—which may include material cybersecurity incidents—while better mitigating the concerns raised above.

Conflict with Confidential Incident Reporting Requirements

The financial sector currently must comply with at least 10 confidential incident reporting requirements.[13] While these rules have different timelines, information requirements, and thresholds for reporting, all seek to leverage rapid incident reports to warn potential downstream victims. The SEC's public disclosure requirement complicates these efforts and shortens the time other agencies have to fully assess an incident and determine its impact prior to public disclosure, thereby compromising the effectiveness of such other agencies' decision-making and undermining coordinated regulatory efforts to enhance national cybersecurity.

When explaining her opposition to the rule, Commissioner Hester Peirce said it "continues to ignore both the limits to the SEC's disclosure authority and the best interests of investors."[14] Beyond

---

https://www.sec.gov/Archives/edgar/data/732717/000000000024009500/filename1.pdf [hereinafter, collectively, the AT&T Letters].

[12] *See, e.g.*, *AlphV files an SEC complaint against MeridianLink for not disclosing a breach to the SEC (2)*, DATABREACHES.NET (Nov. 15, 2023), https://databreaches.net/2023/11/15/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/ [hereinafter the AlphV Incident Article].

[13] U.S. DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023); U.S. DEP'T OF HOUSING & URBAN DEV., FED. HOUSING ADMIN., MORTGAGEE LETTER 2024-10, SIGNIFICANT CYBERSECURITY INCIDENT (CYBER INCIDENT) REPORTING REQUIREMENTS (2024); U.S. DEP'T OF HOUSING & URBAN DEV., GINNIE MAE, APM 24-02, CYBERSECURITY INCIDENT NOTIFICATION REQUIREMENT (2024).

[14] Commissioner Hester M. Peirce, *Harming Investors and Helping Hackers: Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, U.S. SEC. & EXCH. COMM'N. (Jul. 26, 2023),

exceeding the SEC's authority, Commissioner Peirce also raised the SEC's lack of cybersecurity expertise, summarizing this view saying "the new rule looks like a compliance checklist for handling cyber risk, a checklist the SEC is not qualified to write."[15] Indeed, other, more qualified regulators have created reporting and compliance regimes that the rule's incident disclosure requirement undermines.

For example, once the *Cyber Incident Reporting for Critical Infrastructure Act* goes into effect later this year, the Cybersecurity and Infrastructure Security Agency may only have 24 hours to confidentially share threat indicators and defensive measures before an incident is publicly disclosed under the cybersecurity disclosure rule.[16] In fact, this could be reduced to no time at all, if the victim company determines it should file an Item 1.05 8-K ahead of the four business day deadline, as many companies have done, for fear that the Commission or civil litigants will second-guess its timeline for determining materiality and disclosing the incident. This leaves public companies with little to no time to successfully act on those threat indicators and defensive measures before an incident is disclosed to the world, including opportunistic threat actors.

Congress grappled with these concerns when negotiating CIRCIA and made it a priority to protect the information companies share with the government.[17] Consequently, CIRCIA's privacy, use, and liability protections aim to ensure "that entities are encouraged to and feel protected in disclosing cyber incidents" and are not otherwise negatively affected by complying with the law.[18] The SEC should likewise not assume public disclosure takes precedence over other requirements intended to enhance our national and critical infrastructure security.[19]

Complex and Overly Narrow Disclosure Exception

The rule provides a limited exception to its Item 1.05 disclosure requirement in circumstances where the "Attorney General determines that disclosure . . . poses a substantial risk to national security or public safety."[20] Putting aside the insufficient breadth of the exception, the process by which a company must request a disclosure delay is complex and occurs within a rapidly compressed timeframe that negatively impacts both reporting companies and law enforcement.

Under the guidance for requesting a delay, a company must immediately notify the Federal Bureau of Investigation after determining an event is material and submit additional details including when the incident occurred, remediation status, and suspected or confirmed attribution.[21] This information is not only often unavailable, inaccurate, and unclear during the initial stages of incident response, but its collection places yet another urgent administrative requirement on the frontline cyber personnel responsible for remediating a vulnerability and mitigating impacts from ongoing or

---

https://www.sec.gov/newsroom/speeches-statements/peirce-statement-cybersecurity-072623 [hereinafter Peirce Statement].

[15] *Id*.

[16] BPI Comment Letter, at 13.

[17] U.S. S. Comm. on Homeland Sec. & Gov't Affs., Comment Letter on SEC Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 4 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128391-291294.pdf.

[18] *Id*.; 168 CONG. REC. S1149–50 (daily ed. Mar. 14, 2022).

[19] Peirce Statement.

[20] Cybersecurity Disclosure Rule, at 51945.

[21] U.S. DEP'T OF JUSTICE, FED. BUREAU OF INVESTIGATION, CYBER VICTIM REQUESTS TO DELAY SECURITIES AND EXCHANGE COMMISSION PUBLIC DISCLOSURE POLICY DIRECTIVE 1355D (Feb. 28, 2025) [hereinafter Policy Directive 1355D].

subsequent attacks. Those personnel may also be tasked during those initial, critical days with follow up requests focused on obtaining a disclosure exception, rather than containment and remediation efforts.

This exception conflicts with and is significantly narrower in scope than most state data breach laws, which often provide a more general delay for any ongoing law enforcement investigation.[22] Law enforcement exceptions are a commonly accepted legal convention because they give investigators time to identify perpetrators and perform other critical deterrence and response activities. The SEC's circumscribed exception in this case demonstrates its "general refusal to take into account other cyber disclosure laws."[23]

Instead, while a four business day clock ticks, the FBI and DOJ must divert resources and attention from other potentially more pressing national security and law enforcement matters to assess whether an exception is appropriate based on preliminary and likely incomplete information while a company's investigation remains ongoing. The FBI and Department of Justice have acknowledged that the determination process may extend beyond the four business day period by advising companies to initiate the exception process "as soon as possible, even beginning well before the [company] has completed its materiality analysis or its investigation into the incident."[24] Requiring victim companies, the FBI, and DOJ to race through this process during the early stages of incident investigation, before they may be able to reasonably determine whether an exception is desirable or necessary, diminishes the exception's utility and undermines its stated protective function.

Over-Reporting Dilutes Materiality and Reduces Disclosure Utility

Since the rule's implementation, companies have struggled to navigate the boundary between mandatory and voluntary disclosure of cybersecurity incidents, leading to uncertainty and signal dilution. Although the SEC intended Item 1.05 to be triggered only upon a determination of materiality, in practice, companies have at times disclosed incidents prior to making such a determination out of an abundance of caution.

This uncertainty prompted the former Director of the SEC's Division of Corporation Finance to issue a statement addressing apparent market confusion, saying that "Item 1.05 is not a voluntary disclosure, and it is by definition material because it is not triggered until the company determines the materiality of an incident."[25] He further warned that disclosing immaterial incidents or those not yet assessed for materiality under Item 1.05 "could be confusing for investors."[26] These clarifications were necessary because, in the months leading up to the statement, many companies disclosed incidents under Item 1.05 while stating that the incidents were unlikely to have certain material impacts, potentially undermining the purpose of Item 1.05 and flooding investors with immaterial or incomplete information.

Following the statement, the pace and character of disclosure shifted meaningfully. Many companies redirected filings to Item 8.01, leaving investors to subjectively divine the difference in degree

[22] *Security Breach Notification Laws*, NAT'L. CONF. STATE LEGISLATURES (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.
[23] Peirce Statement.
[24] Policy Directive 1355D.
[25] Gerding Statement.
[26] *Id*.

of a company filing under Item 1.05 or 8.01. While prior to SEC's clarifying statement, 17 companies disclosed cybersecurity incidents under Item 1.05, in contrast, only nine such disclosures occurred after the statement through year-end 2024—a marked decline. At the same time, disclosures under Item 8.01 surged from six in 2024 prior to the statement, to 28 in the months following.

However, despite the clarification statement, confusion and defensive filings have persisted. For example, in the correspondence between AT&T Inc. and SEC staff over AT&T's July 12, 2024, 8-K filing, the staff questioned AT&T's choice to disclose the incident under Item 1.05, given that AT&T had not yet determined the material impacts of the incident. In the subsequent correspondence, the staff disagreed with AT&T's position that an incident could be "material" without having any disclosable material impacts.[27] In response to AT&T's decision to disclose information it believed was material and important for investors, the staff's position counterintuitively encourages companies to refrain from disclosing cybersecurity incidents under Item 1.05 unless they also speculate as to the "reasonably likely material impact" of the incident. Overall, of the 32 companies that have filed under Item 1.05, only nine identified a material impact in their initial disclosures, and just two more did so in amended filings. Rather than providing clarity, the inconsistent use of Items 1.05 and 8.01, and Item 1.05's requirement to speculate regarding future material impacts, injects uncertainty into the market and undermines the objective of standardized, decision-useful disclosure.

Weaponized By Ransomware and Other Cyber Criminals

In November 2023, after the SEC adopted the rule, ransomware group AlphV took the unprecedented step of reporting its own victim, MeridianLink, to the SEC as a ransom payment extortion tactic.[28] In its formal submission, AlphV stated, "we want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules."[29] AlphV went further, reporting that "it has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K."[30]

AlphV's action is not an isolated case but a harbinger of a growing trend where cybercriminals leverage regulatory requirements to further their malicious objectives. We are aware of other instances where threat actors have deployed similar pressure on victims and referenced the incident disclosure requirement in connection with threats and demands. This tactic not only exacerbates the financial and operational damage to the victim companies but also undermines the purpose of the disclosure rule by turning it into leverage for extortion. On average, ransomware attacks cost victims several million dollars and some estimate these attacks will cost victims $275 billion annually by 2031.[31] Given the pervasiveness of ransomware attacks, it is misguided to provide cybercriminals with an additional means to inflict financial harm on victim companies.

---

[27] The AT&T Letters.

[28] The AlphV Incident Article.

[29] *Id.*

[30] *Id.*

[31] Luke Dembosky and Jordan Rae Kelly, *Ransomware in the financial sector*, ABA BANKING J. (Aug. 29, 2024), https://bankingjournal.aba.com/2024/08/ransomware-in-the-financial-sector/; Steve Morgan, *Global Ransomware Damage Costs Predicted to Exceed $275 Billion By 2031*, CYBERCRIME MAG. (Apr. 2, 2025), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

In addition to these tactics, in the event that a company does publicly disclose an incident under Item 1.05 while an incident is ongoing, the company may face additional attacks by new threat actors seeking to exploit an unresolved vulnerability or take advantage of a company's weakened cyber defenses while attention and resources are focused on the initial attack. Item 1.05 thus puts companies in a difficult situation: either face extortion threats by ransomware cybercriminals if the company does not publicly disclose an incident under Item 1.05 or invite a new wave of cyber attacks by publicly broadcasting that a company's cyber defenses may be vulnerable or overextended.

In her dissenting statement on the rule, SEC Commissioner Peirce predicted these risks, noting that the disclosure requirements "seem designed to better meet the needs of would-be hackers rather than investors' need for financial information."[32] Rescinding the requirement that companies publicly disclose ongoing cybersecurity incidents will help eliminate this unnecessary exposure.

Insurance and Liability Implications

Mandating the public disclosure of a cybersecurity incident before it is fully investigated or remediated creates significant and potentially costly legal exposure for registrants, particularly by mandating disclosure based on preliminary information, including in some cases information available only from third parties, that may unintentionally be incomplete or inaccurate, and therefore may inadvertently misinform investors and fuel market volatility.

Premature filings under Item 1.05 may later be used by plaintiffs' attorneys in securities class actions or leveraged by insurers to deny coverage on grounds that the risk was "known" or inadequately mitigated. Moreover, because the Form 8-K disclosure is a "filing" (not furnished), it may expose registrants to costly litigation, including under Section 18 of the Securities Exchange Act of 1934, which creates liability for any false or misleading statement of material fact made in a filed document, unless the filer can prove good faith and lack of knowledge of the inaccuracy, and Section 11 of the Securities Act of 1933, which imposes strict liability for material misstatements and omissions in a registration statement.

Chilling Effect on Internal Communications and External Information Sharing

Stemming from the liability risks, in part, the incident disclosure requirement also risks creating a chilling effect on candid internal communications and routine, external information sharing.[33] Litigation risks, along with the threat that the SEC could investigate a disclosure decision, heighten the risk for extensive discovery of communications. We are aware of recent instances where the enforcement staff of the SEC requested extensive records of all communications about the incident, which, made during a rapidly evolving situation, risk being unfairly scrutinized in hindsight. This incentivizes legal departments and incident response teams to limit internal correspondence or

[32] Peirce Statement.

[33] The former Director of the SEC's Division of Corporation Finance issued a clarifying statement stating that Item 1.05 should not chill information sharing; however, this clarification has proven ineffective in practice, as industry participants continue to report hesitancy in sharing information due to concerns about regulatory scrutiny and potential liability. *See* Erik Gerding*, Selective Disclosure of Information Regarding Cybersecurity Incidents,* U.S. SEC. & EXCH. COMM'N. (June 20, 2024), https://www.sec.gov/newsroom/whats-new/gerding-cybersecurity-incidents-06202024.

documentation of internal deliberations or assessments for fear that such materials may later be misconstrued as bearing on materiality or create litigation risk.

For these same reasons, the incident disclosure rule is having a chilling effect on the cybersecurity incident-related information companies share externally to private and public sector stakeholders. The financial sector takes seriously its opportunities to report incidents to law enforcement and to share information with peers and industry groups—such as early-stage threat assessments, hypotheses about attacker behavior, or preliminary forensic findings—to support cybersecurity response and defense measures. However, since the incident disclosure requirement came into effect, we have seen greater hesitance from companies to share this critical information, out of a concern the information disclosed will later be misconstrued as bearing on materiality, or the misconception that information about significant cybersecurity threats cannot be shared ahead of a public disclosure. For instance, SEC subpoenas regarding disclosures have requested all information provided to another government agency, including the FBI, with whom companies often share information about incidents or other cyber threats. We have seen this restricted information exchange during a recent, large-scale incident, where a prominent technology company declined to share detailed, technical information with industry partners to help other companies defend against similar attacks, instead directing them to the non-technical information included in its 8-K filing.

Over time, this could erode the quality of cross-functional communication between cybersecurity professionals, legal counsel, compliance, and management, cross-industry communication with peer companies, as well as proactive outreach to law enforcement. Rather than encouraging transparency, the rule may paradoxically incentivize opacity and over-cautious communication, degrading both cybersecurity readiness and disclosure quality.

Return to a More Streamlined and Appropriate Disclosure Framework

The Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule created a regime prioritizing cybersecurity risk above many other risks. Commissioner Mark Uyeda, dissenting from the rule, noted precisely this issue, saying that the amendments "swing a hammer at the current regime and create new disclosure obligations for cybersecurity matters that do not exist for any other topic."[34] This includes disclosures for risks related to acquisitions, product development, regulatory approvals, and supply chain management—many of which could have a more significant effect on a company's financial performance.[35] Commissioner Uyeda noted further that "no other Form 8-K event requires such broad forward-looking disclosure that needs to be constantly assessed for a potential amendment."[36] For instance, a company's 8-K disclosure obligations following a substantial acquisition contains no requirement to speculate on its "impact, or reasonably likely impact, on the company."[37] Rescission of Item 1.05 would correct this errant swing of the SEC's hammer, and reinstate a principles-based disclosure regime which allows public companies to treat the risks relating to cybersecurity similar to other material financial, operational, and governance risks.

---

[34] Commissioner Mark T. Uyeda, *Statement on the Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, U.S. SEC. & EXCH. COMM'N. (Jul. 26, 2023), https://www.sec.gov/newsroom/speeches-statements/uyeda-statement-cybersecurity-072623.
[35] *Id*.
[36] *Id*.
[37] *Id*.

By rescinding Item 1.05, the SEC would not eliminate the ability or obligation for registrants to evaluate and appropriately disclose material information about cybersecurity risks to investors. As one means for doing so, registrants have historically used, and continue to use, Item 8.01 to voluntarily disclose cybersecurity incidents. Item 8.01 provides registrants with an option to voluntarily disclose events that a company deems important to investors but are otherwise not affirmatively required to be disclosed under other items of Form 8-K. Under a principles-based disclosure regime, rather than prescriptive and overly burdensome Item 1.05 requirements, registrants would again be able to appropriately determine whether and when to disclose significant cybersecurity incidents in order to provide timely and decision-useful information for investors. Moreover, registrants would still be required to disclose material information about cybersecurity risks and incidents. Since 2011, the Commission has made clear that companies should consider the materiality of cybersecurity risks and incidents when preparing disclosure required in registration statements, periodic reports, and current reports, including the disclosure contained in risk factors, management's discussion and analysis of financial condition and results of operations, description of business, and financial statements, as well as disclosure pertaining to legal proceedings, disclosure controls and procedures, and corporate governance.[38]

The rescission of Item 1.05 also would not absolve registrants of their obligations under Regulation FD. Registrants would still be required to disclose material nonpublic information to all investors simultaneously, ensuring that no group of investors is unfairly advantaged.

This pre-existing disclosure framework relieves the pressure of Item 1.05's four business day deadline, leaving companies better positioned to contain incidents, conduct thorough investigations to gain a more complete and accurate understanding of the incident, mitigate harms, and pursue remediation efforts. In turn, we believe disclosures under such a principles-based regime will contain more meaningful, decision-useful information for investors.

Accordingly, a return to the SEC's longstanding principles-based approach—whereby companies assess disclosure obligations based on existing periodic disclosure requirements and longstanding materiality standards[39]—would offer a clearer, more consistent, and investor-useful framework. Rather than compelling disclosure of preliminary and speculative information about incidents under Item 1.05, the SEC's time-tested, established approach empowers companies to disclose information that is meaningful, reliable, and material. This, in turn, balances the need for investors to receive timely and relevant information without imposing undue burdens on companies, thereby enhancing the overall effectiveness of the regulatory framework, and supporting the SEC's mission to facilitate capital formation and protect investors.

Conclusion

For the reasons set forth above, we respectfully request that the SEC rescind the Form 8-K Item 1.05 incident reporting requirements, and the parallel reporting requirements applicable to Form 6-K, from its Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule to address

[38] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166 (Feb. 26, 2018); *CF Disclosure Guidance: Topic No. 2—Cybersecurity*, U.S. SEC. & EXCH. COMM'N (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[39] *See* 17 C.F.R. § 240.12b-20 (requiring inclusion of "further material information…as may be necessary to make the required statements, in light of the circumstances under which they are made not misleading.").

the significant risks and burdens imposed on registrants by the rule. We are committed to working with you to develop a balanced cyber disclosure regime that acknowledges national security realities while not losing sight of the SEC's investor protection mandate. If you have any questions or would like to discuss these comments further, please reach out to John W. Carlson at jcarlson@aba.com, Heather Hogsett at heather.hogsett@bpi.com, Melissa MacGregor at mmacgregor@sifma.org, Anjelica Dortch at anjelica.dortch@icba.com, and Michelle Meertens at mmeertens@iib.org.

Sincerely,

/s/ John W. Carlson
John W. Carlson
Senior Vice President, Cybersecurity Regulation & Resilience
American Bankers Association

/s/ Heather Hogsett
Heather Hogsett
Senior Vice President, Dep. Head of BITS
Bank Policy Institute

/s/ Melissa MacGregor
Melissa MacGregor
Deputy General Counsel & Corporate Secretary
Securities Industry and Financial Markets Association

/s/ Anjelica Dortch
Anjelica Dortch
Vice President, Operational Risk & Cybersecurity Policy
Independent Community Bankers of America

/s/ Michelle Meertens
Michelle Meertens
Deputy General Counsel
Institute of International Bankers