April 10, 2026

Via Electronic Mail

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

Re: Comment on Reforming Regulation S-K (File No. CLL-15) – Regulation S-K Item 106 and Cybersecurity Disclosure

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] appreciate the opportunity to provide comments in response to Chair Atkins's request for

[1] The American Bankers Association is the voice of the nation's $25.3 trillion banking industry, which is composed of small, regional, and large banks that together employ over 2 million people, safeguard $20.1 trillion in deposits, and extend $13.5 trillion in loans.

[2] The Bank Policy Institute ("BPI") 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. BPI 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, 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] The Securities Industry and Financial Markets Association ("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 nearly 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.

[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 credit for U.S. borrowers and comprise the majority of U.S. primary dealers. These institutions also enhance the

public input on reforming Regulation S-K. Our members are subject to extensive cybersecurity oversight and incident-reporting regimes administered by prudential regulators and federal agencies, in addition to the public disclosure requirements of the Commission's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule.[6] This letter focuses on Item 106 of Regulation S-K and the related cybersecurity incident disclosure mandate on Form 8-K, Item 1.05.[7]

We welcome the Commission's comprehensive review of Regulation S-K and its effort to restore a materiality-centered, principles-based disclosure framework whereby companies assess disclosure obligations based on longstanding materiality standards. As noted in the recently released Cyber Strategy for America, cyber regulations should be streamlined to "reduce compliance burdens, address liability, and better align regulators and industry globally."[8] As part of the Commission's review, we urge the Commission to rescind Item 106.

We believe Item 106 places outsized weight on one risk type and requires disclosure of operational details inconsistent with a principles-based framework. Rescission of Item 106 would streamline disclosure and "eliminat[e] both the burdensome and the impractical," in alignment with Chair Atkins's strategy for the Commission's regulatory frameworks.[9] In the event the Commission does not rescind Item 106, we recommend that the Commission narrow and refocus Item 106 so that it elicits concise, decision-useful and materiality-centered information about cybersecurity risks and risk management, without burying investors in immaterial detail. In addition, as part of the Commission's review, we urge the Commission to rescind Form 8-K, Item 1.05. We believe that the pre-existing principles-based disclosure framework (including Form 8-K, Item 8.01 and periodic reporting requirements) adequately addresses disclosure of material cybersecurity incidents, as described in the joint petition for rulemaking submitted by our organizations last year.[10]

---

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

[7] The recommendations in this letter should apply equally to foreign private issuers ("FPIs"). FPIs are subject to cybersecurity governance and risk management disclosure requirements through Form 20-F Item 16K, which incorporates the substance of Regulation S-K Item 106. Similarly, FPIs are required to furnish on Form 6-K material cybersecurity incident disclosures, similar to the disclosure mandated by Form 8-K, Item 1.05. Any actions taken by the Commission to implement the recommendations herein should therefore be reflected in the parallel disclosure requirements in Form 20-F Item 16K and Form 6-K.

[8] The White House, President Trump's Cyber Strategy for America (Mar. 6, 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf.

[9] Chair Paul S. Atkins, U.S. Sec. & Exch. Comm'n, *Prepared Remarks Before SEC Speaks* (Mar. 19, 2026), https://www.sec.gov/newsroom/speeches-statements/atkins-remarks-sec-speaks-031926-prepared-remarks-sec-speaks.

[10] American Bankers Assoc., Bank Policy Institute, Securities Industry and Financial Markets Assoc., Indep. Cmty. Bankers of America, and Inst. of Int'l Bankers, Petition for Rulemaking on the Cybersecurity Rick Management, Strategy, Governance, and Incident Disclosure Rule (May 22, 2025), https://bpi.com/wp-content/uploads/2025/05/Joint-Financial-Trades-Final-Petition-for-Rulemaking-on-Cybersecurity-Risk-Management-Strategy-Governance-and-Incident-Disclosure-Rule_.pdf [hereinafter Petition for Rulemaking].

I. The Commission Should Rescind Item 106

In 2022, our associations explained that the proposed cybersecurity rules raised serious policy and practical concerns, including the following: (1) the risk that bespoke, topic-specific line items for cybersecurity incidents would privilege one type of risk over others in a way that is inconsistent with the Commission's longstanding, principles-based regime[11] and (2) security risks from prescriptive disclosures about cybersecurity. Although the Commission acknowledged many of the comments it received in the final rule, it did not resolve several issues with Item 106's requirements, including the concerns raised by our associations. These issues now warrant reconsideration in the context of Regulation S-K reform, particularly as compliance with Item 106's disclosure requirements has negatively impacted the members of our associations. For example, our member financial services firms devote significant attention and resources away from other important priorities to complying with Item 106's detailed disclosure requirements—leaving less time for other strategic security initiatives to fortify firm defenses. At the same time, the growing patchwork of overlapping cybersecurity rulemakings across federal agencies and state regimes further risks the diversion of finite resources away from proactive threat detection and toward prescriptive compliance exercises. Smaller and mid-sized financial services firms, in particular, find compliance challenging given their more limited resources.

A. Item 106 Puts Outsized Weight on One Risk Type

Chair Atkins has rightly observed that Regulation S-K has grown from "the size of a gym locker to the size of an artificial-intelligence data center," forcing investors to sift through an "avalanche of immaterial information."[12] Cybersecurity is a salient risk for many registrants, but it is one among many operational, legal, strategic, and other risks that, where material, are already subject to disclosure under Regulation S-K. Cybersecurity can also be an underlying factor that amplifies other risks. By creating a stand-alone Item 106 with detailed line-item requirements on risk management processes, governance, and incident history, the Commission has adopted a one-size-fits-all approach that singles out cybersecurity for more prominent disclosure than other risks, including broader technology risks, that may be equally or more consequential for certain registrants. Moreover, a stand-alone disclosure requirement risks obscuring how cybersecurity risk manifests within a registrant's broader risk profile by potentially disaggregating related risk disclosure and requiring immaterial detail. Since cybersecurity risk is inherently integrated across a range of risk categories, presenting it separately from other risks less effectively conveys material information to investors. As Commissioner Uyeda observed, the

[11] 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; Securities Industry and Financial Markets Assoc., Comment Letter on SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128347-291108.pdf.

[12] Chair Paul S. Atkins, *Statement on Reforming Regulation S-K*, U.S. SEC. & EXCH. COMM'N (Jan. 13, 2026), https://www.sec.gov/newsroom/speeches-statements/atkins-statement-reforming-regulation-s-k-011326.

cybersecurity rules "swing a hammer at the current regime and create new disclosure obligations for cybersecurity matters that do not exist for any other topic."[13]

Instead of a separate line-item requirement, the Commission has previously recognized that cybersecurity risks, like other risks, should be disclosed under existing Regulation S-K requirements,[14] including Items 101, 103, 105, 303, and 407, which require disclosure of material aspects of a registrant's business, risks, legal proceedings, financial condition and results of operations, and governance structures. Furthermore, Section 10(b), Rule 10b-5, and Rule 12b-20 under the Securities Exchange Act of 1934, as amended (the "Exchange Act"), along with Rule 408 under the Securities Act of 1933, as amended (the "Securities Act"), require disclosure of material information to ensure that statements made are not materially misleading, which may include disclosure of material cybersecurity risks and how cybersecurity relates to other aspects of a registrant's business. A separate, prescriptive Regulation S-K requirement is not necessary to elicit disclosure of material cybersecurity information and, as noted above, may place undue prominence on one particular risk type. Instead, a materiality-driven, principles-based framework should allow registrants to exercise judgment about whether, how, and where such information is most meaningfully disclosed.

The Commission has consistently taken a principles-based approach and not imposed separate line-item requirements in analogous contexts. Most recently, Chair Atkins declined to mandate specific disclosures for artificial intelligence risks, emphasizing that the Commission should not impose prescriptive, topic-specific disclosure requirements where existing principles-based rules already capture material information.[15] The same reasoning applies here—cybersecurity risks should be appropriately addressed within the Commission's existing principles-based Regulation S-K requirements rather than a separate topic-specific disclosure requirement. Cybersecurity risks, like other risks, should be disclosed when they are material and in the context that is most meaningful to investors—such as disclosing material risk factors for a registrant's business or the registrant's governance and management oversight structures—not through a stand-alone, prescriptive disclosure requirement.

B. Item 106 Requires Disclosure of Operational Detail That May Create Security Risks Without Providing Commensurate Investor Benefit

In 2022, we cautioned that prescriptive disclosure about the "nature or status of remediation activities, including changes to cybersecurity policies and procedures,"[16] as well as granular discussion of

---

[13] 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.

[14] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018).

[15] Chair Paul S. Atkins, *Remarks at the Investor Advisory Committee Meeting,* U.S. Sec. & Exch. Comm'n (DEC. 4, 2025), https://www.sec.gov/newsroom/speeches-statements/atkins-remarks-iac-120425.

[16] 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 6 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128336-291093.pdf.

third-party oversight mechanisms,[17] could unintentionally provide a roadmap for adversaries while adding little informational value for investors. The Commission responded by deleting some of the most detailed prescriptive requirements,[18] but Item 106 still directs registrants to describe their "processes" for "assessing, identifying, and managing material risks from cybersecurity threats"[19] and to outline management's role in assessing and managing those risks[20]—a level of detail not required for any other risk type under Regulation S-K.

Requiring registrants to describe in detail how they detect, investigate, and remediate cyber incidents, or how they monitor and manage third-party cybersecurity risks, has the potential to reveal operational practices that sophisticated threat actors could use to tailor their attacks, probe for gaps, or circumvent safeguards. For example, many registrants disclose the role of officers responsible for specific cybersecurity risk management processes, and such disclosures may create an easily searchable roadmap for threat actors to carry out phishing and social-engineering attacks, including impersonating company officers. Similarly, requiring registrants to disclose whether they maintain processes to oversee third-party risks may reveal third- and fourth-party vulnerabilities that could affect the security of the registrant's systems.

The current administration has recognized these security risks and, in March 2026, cautioned that "cyber defense should not be reduced to a costly checklist that delays preparedness, action and response."[21] In practice, however, Item 106 encourages exactly this—a detailed recitation of frameworks, committees, and processes—rather than a concise discussion of how cybersecurity fits into the registrant's overall risk profile and strategy.

Item 106 compels disclosure of operational detail that goes beyond what is necessary for investors to assess material risks and requires information that is more appropriately shared confidentially with regulators. In highly regulated sectors such as financial services, supervisory frameworks already require robust cyber risk management programs and detailed, confidential reporting to prudential regulators. Additional confidential reporting obligations to the Cybersecurity and Infrastructure Security Agency ("CISA") are forthcoming. Similarly, other critical infrastructure sectors, including energy, telecommunications, and healthcare, are subject to cybersecurity regulations that overlap with Item 106. Rather than filling a gap, Item 106 adds to an already crowded and fragmented reporting environment, increases compliance burdens, and risks eroding a firm's cybersecurity posture without meaningfully improving the "total mix"[22] of information available to investors.

---

[17] Securities Industry and Financial Markets Assoc., Comment Letter on SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 20 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128347-291108.pdf.

[18] Cybersecurity Disclosure Rule, at 51910.

[19] 17 C.F.R. § 229.106(b)(1).

[20] *Id.* at § 229.106(c)(2).

[21] The White House, President Trump's Cyber Strategy for America (Mar. 6, 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf.

[22] TSC Industries v. Northway, Inc., 426 U.S. 438, 449 (1976).

In addition, several commenters on the original proposal noted that the prescriptive nature of the Item 106 requirements appears, at least in part, to dictate a registrant's approach to cybersecurity risk management and governance rather than simply eliciting information material to investors. This further risks providing bad actors with a roadmap of internal cybersecurity functions to exploit across many companies. In practice, there has been notable convergence in Item 106 disclosures, resulting in similar descriptions of cybersecurity risk management frameworks and processes, reporting lines, incident response approaches, and governance structures across registrants. This convergence not only fails to provide decision-useful information to investors but also obscures truly material, company-specific risks and practices, while still providing operational detail that itself creates security risks. This convergence may, at least in part, be driven by companies adopting internal processes responsive to Item 106 requirements and mirroring those disclosed by peer companies, illustrating the potential for disclosure requirements to incentivize behavior not necessarily aligned with the best security interests of the company. As the Commission stated in its 2018 guidance, "Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors."[23]

The Item 106 disclosure requirements are inconsistent with the Commission's current effort to streamline Regulation S-K and refocus it on what truly matters to reasonable investors, as well as the Commission's long-standing guidance for cybersecurity disclosure. Rescinding Item 106 as part of reforming Regulation S-K would not weaken investor protections because, as discussed above, cybersecurity would be subject to existing applicable Regulation S-K disclosure requirements. Instead, recission would provide investors with more decision-useful information and realign cybersecurity disclosure with the Commission's core philosophy of materiality-centered, principles-based disclosure.

C. Item 106 Conflicts with the Administration's Deregulatory Agenda

Item 106 is also in tension with the administration's broader federal deregulation agenda, as stated in Executive Order 14192—Unleashing Prosperity Through Deregulation, which directed agencies to reduce unnecessary regulatory burdens.[24] Compliance with Item 106 requires significant resources, which disproportionately impacts smaller companies with more limited resources. Moreover, beyond domestic cybersecurity regulatory regimes, many registrants also operate internationally and are subject to cybersecurity reporting obligations across various foreign jurisdictions that overlap with Item 106, further complicating registrants' compliance efforts. As the Commission undertakes its review of Regulation S-K, retaining Item 106 in its current form would be inconsistent with its mandate to streamline regulation and reduce compliance burdens. Accordingly, for the reasons discussed above, we urge the Commission to rescind Item 106.

II. If Not Rescinded, Item 106 Should Be Narrowed and Clarified

In the event that the Commission does not rescind Item 106, we recommend that the Commission narrow and clarify Item 106 so that it elicits concise, decision-useful, and materiality-

[23] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8169 (Feb. 26, 2018).

[24] Exec. Order No. 14,192, Unleashing Prosperity Through Deregulation, 90 Fed. Reg. 9065 (Feb. 6, 2025)

centered information about cybersecurity risks and risk management without burying investors in immaterial detail.

A. Narrow and Clarify the Overly Broad Definition of "Cybersecurity Incident"

Item 106 defines "cybersecurity incident" as "an unauthorized occurrence, or a series of related unauthorized occurrences, 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."[25] That formulation remains broader than necessary to capture incidents that have, or are reasonably likely to have, material effects and broader than leading federal benchmarks such as the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA")[26] and the prudential banking regulators' Computer-Security Incident Notification Rule.[27] We recommend that the Commission revise the definition of "cybersecurity incident" to substantially align with the definition of "computer-security incident" and "notification incident" under the Computer-Security Incident Notification Rule.

As noted in our prior letters, it remains unclear what constitutes a "series of related unauthorized occurrences," and as such, the Commission should strike this language from the "cybersecurity incident" definition. In particular, Item 106 does not specify whether this phrase refers to similar types of attacks carried out by the same threat actor, multiple similar attacks carried out by different actors, or incidents that share common characteristics but occur over an extended period of time. It is also unclear over what timeframe separate occurrences could reasonably be aggregated and considered part of a "series," including whether incidents occurring over the course of a year or longer could fall within this definition. In practice, this ambiguity creates uncertainty about whether recurring but routine events should be treated as individually immaterial incidents or as a potentially material "series" of incidents requiring disclosure. Striking a "series of related unauthorized occurrences" from the definition would eliminate this ambiguity and promote more consistent application of the rules.

In addition, in prior comment letters,[28] we explained that the term "jeopardizes" compels disclosure of cybersecurity events that may never result in actual loss or operational impact, effectively pressuring registrants to speculate about possible future impacts of incidents in connection with Item 106's requirements. We urged the Commission to conform its standard to CIRCIA's "substantial loss of confidentiality, integrity, or availability … or a serious impact on the safety and resiliency of operational

[25] 17 C.F.R. § 229.106(a).
[26] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 49, 1038 (2022).
[27] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66, 424 (2021).
[28] 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 18 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128336-291093.pdf; Securities Industry and Financial Markets Assoc., Comment Letter on SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 8 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128347-291108.pdf.

systems and processes"[29] threshold, which anchors the trigger in an actual, observable impact rather than conjectural risk. The final rule did not adopt that recommendation.[30] Instead, it retained the "jeopardizes" formulation, thereby leaving registrants to parse an expansive definition that sweeps in cybersecurity incidents well beyond the scope of other cyber regulations. It also requires registrants to make potentially immaterial public disclosures that could provide bad actors with a roadmap of the company's cyber vulnerabilities.

The same is true of "information systems," which is defined in Item 106 to include "information resources, owned or used by the registrant, including physical or virtual infrastructure."[31] As we noted previously,[32] sweeping "physical" infrastructure into the definition, without clarifying that it refers only to information technology resources used for the transmission, processing, or storage of electronic data, risks pulling a wide range of operational events into the cybersecurity disclosure bucket, including physical or technical failures that may be wholly unrelated to cybersecurity attacks. Similarly, there is also no such clarification for virtual infrastructure. The inclusion of systems "used by the registrant…for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations" potentially sweeps in third-party service providers storing a registrant's data for discrete, limited purposes. As a result, the "information systems" definition is ambiguous on which third-party incidents must be disclosed by the registrant, and should be narrowed to address only those systems within the registrant's control. In general, the ambiguity and breadth of the "cybersecurity incident" and the "information systems" definitions dilute the value of Item 106 disclosures and complicate coordination with other cybersecurity reporting requirements keyed to more focused technology concepts.

From a drafting perspective, these are solvable problems. Narrowly drawn definitions will better serve the Commission's stated objective by eliciting concise, decision-useful, and materiality-centered information that a reasonable investor would consider important without burying investors in immaterial detail. Accordingly, if the Commission does not rescind Item 106, we recommend that the Commission narrow and clarify the definitions of "cybersecurity incident" and "information systems" in Item 106.

In particular, the Commission should revise Item 106 so that only those cybersecurity incidents meeting the threshold of a "notification incident" under the Computer-Security Incident Notification Rule are reportable. The Computer-Security Incident Notification Rule defines a "computer-security incident" as "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."[33] The rule further clarifies that a "notification incident" is one that meets the definition above and *also* has

[29] 6 U.S.C. § 681b(c)(2)(A)(i).
[30] *See* Cybersecurity Disclosure Rule, at 51916.
[31] 17 C.F.R. § 229.106(a).
[32] 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 18 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128336-291093.pdf.
[33] *See supra* note 27, at 66, 425.

"materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's: (i) ability to carry out banking operations, activities or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States."[34]

If the Commission does not rescind Item 106, we believe Item 106 should conform to the framework in the Computer-Security Incident Notification Rule adopted by the prudential banking agencies and only require disclosure of cybersecurity incidents causing material disruption or degradation—i.e., notification incidents. The "computer-security incident" definition in that rule provides a more measurable threshold than Item 106's expansive "jeopardizes" formulation by limiting the scope of reportable incidents to those resulting "in *actual harm* to the confidentiality, integrity or availability of an information system."[35] With appropriate modification, the Computer-Security Incident Notification Rule's definitions could be adapted for all registrants, not only banking organizations. Instituting an impact-based standard for Item 106 would promote consistency across federal regulatory regimes and reduce unnecessary compliance burdens.

B. Refocus Item 106 on Material Information, Not Operational Detail

Additionally, for the reasons discussed above, Item 106(b) and (c) should be streamlined so that registrants are not expected to disclose granular details of their cybersecurity programs, controls, or procedures when such detail is not necessary for a reasonable investor to understand the material risks to the business. Instead, Item 106 should require registrants to describe, to the extent material, (i) how they integrate cybersecurity risk into enterprise risk management and strategy and (ii) how the board of directors oversees those risks rather than inventorying specific processes. The Commission should also remove the Item 106(b) requirement to provide specific disclosures regarding the effects of cybersecurity threats and allow registrants to determine whether such effects are material risks otherwise disclosable under Regulation S-K Item 105. Refocusing Item 106 on material information rather than operational detail would bring Item 106 closer to the Commission's 2018 guidance, which recognized that overly detailed cybersecurity disclosures can themselves create security risks. The 2018 guidance also emphasized the Commission's long-standing expectation that companies avoid generic disclosure and instead adopt a tailored "company-by-company approach [to disclosure] that allows relevant and material information to be disseminated to investors."[36]

[34] *Id.*
[35] *Id*.
[36] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8169 (Feb. 26, 2018).

III. The Commission Should Rescind Form 8-K, Item 1.05

As noted above, last May, we petitioned the Commission to rescind Item 1.05 and the corresponding Form 8-K requirements.[37] We will not restate that petition in full, but several points bear emphasis in the context of Regulation S-K reform as Item 1.05 of Form 8-K imposes substantially similar issues to Item 106 but with additional disclosure burdens that render it especially problematic.

A. Item 1.05 Provides Limited Time for Assessment and Action Before Public Disclosure is Mandated

Financial institutions currently must navigate at least 10 separate confidential federal cyber incident reporting requirements, including those administered by prudential banking regulators.[38] Despite differences in timing, information requirements, and reporting thresholds, these confidential reporting requirements all share a common objective of enabling and prioritizing coordinated defense, not public attribution.

By mandating public disclosure of material incidents within four business days of a materiality determination—often while the incident is ongoing—Item 1.05 compresses the window in which financial institutions and agencies, including CISA, can assess the threat and disseminate indicators of compromise before adversaries are alerted. In doing so, Item 1.05 disclosure can divert a registrant's resources, interfere with incident response efforts, and limit the ability of both registrants and government partners to contain and mitigate active threats. These challenges are compounded by the need to quickly engage outside counsel to assess incidents and disclosure obligations, as well as, in many cases, to consult with insurers before making disclosure decisions—steps that can introduce further delay. Premature filings under Item 1.05 may later be leveraged by insurers to deny coverage on grounds that the risk was "known" or inadequately mitigated. Item 1.05 also exposes investors to premature and potentially misleading disclosures by requiring registrants to disclose incomplete information about rapidly evolving incidents.

As our previous petition explained, this timing tension "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."[39] Congress confronted these issues in CIRCIA and built strong confidentiality and liability protections precisely to encourage timely, candid reporting.[40] Public disclosure under Item 1.05 should not override Congress's policy judgment on the value and timing of confidential incident reporting. These timing concerns can be

[37] Petition for Rulemaking at 2.

[38] 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).

[39] Petition for Rulemaking at 3.

[40] 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.

mitigated by rescinding Item 1.05 and allowing registrants to rely on the existing disclosure framework, including Form 8-K, Item 8.01, which provides flexibility to disclose incidents when they are determined to be material without imposing a rigid deadline.

B. The Delay Mechanism is Too Narrow and Complex

Item 1.05 includes a limited exception under which the Attorney General may determine that disclosure would pose a substantial risk to national security or public safety.[41] As the Department of Justice (the "DOJ") and the Federal Bureau of Investigation (the "FBI") have since explained, invoking that exception requires the victim company to contact the FBI, the U.S. Secret Service, CISA, the Department of War, or another sector risk management agency promptly upon determining materiality and provide detailed information about the incident, often during the earliest and least certain stages of investigation.[42] The DOJ and the FBI, in coordination with relevant federal agency stakeholders, must then make a rapid assessment on whether a disclosure delay is appropriate based on preliminary information—expending resources to comply within the four-business-day window while both law enforcement and the victim company are still triaging the event. Furthermore, lengthy government shutdowns in recent years, during which federal agencies have operated at a limited capacity, introduce potential logistical difficulties to the already time-sensitive delay mechanism dependent on prompt agency coordination.

This complex process is substantially narrower than the law-enforcement delay provisions in most state data-breach statutes[43] and imposes additional burdens on companies without reliably preventing harmful disclosures, as evidenced by our experience over the last 18 months. This process is particularly burdensome for smaller and resource-constrained registrants often lacking the internal capacity and immediate resources to navigate the Item 1.05 delay mechanism within the required timeframe.

Additionally, requiring coordination with the DOJ, the FBI or other agencies at this early stage complicates decision-making during remedial efforts for ongoing cybersecurity incidents, as registrants must balance public disclosure requirements against how best to secure their organizations. These process demands fall unevenly across registrants, with larger entities better positioned to absorb the associated legal, operational, and financial burdens than smaller registrants.

C. Item 1.05 Has Produced Confusion, Over-Reporting and Dilution of Informational Value

Despite multiple clarifying statements, Item 1.05 has generated persistent confusion about when a cybersecurity incident must be reported under that item, may be reported under Item 8.01, or need not be reported on Form 8-K at all. Registrants, understandably reluctant to risk second-guessing, have sometimes filed Item 1.05 reports before completing a materiality analysis or while explicitly

[41] Cybersecurity Disclosure Rule, at 51945.

[42] 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).

[43] *Security Breach Notification Laws*, NAT'L. CONF. STATE LEGISLATURES (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.

stating that no material impacts were expected, diluting the informational value of Item 1.05 disclosure. In May 2024, the former Director of the Commission's Division of Corporation Finance felt compelled to reiterate that Item 1.05 is not a "voluntary" disclosure item, that it is triggered only by material incidents, and that using Item 1.05 for immaterial events could confuse investors.[44]

The data observed since that statement underscores the point that Item 1.05 is unnecessary and should be rescinded. Since the Commission's clarifying statement, Item 8.01 cyber-related filings have surged to approximately 50, while Item 1.05 cyber-related filings more than halved in 2025 compared to the previous year, indicating the growing tendency for companies to make cyber-related filings pursuant to Item 8.01 instead of Item 1.05. This shift suggests that, in practice, registrants are relying on existing disclosure requirements to communicate cyber incidents to the public, calling into question the necessity of a separate Item 1.05 requirement. Further, as demonstrated by the mix of Item 1.05 and Item 8.01 disclosures, Item 1.05 has created confusion about whether a cybersecurity incident could be material without resulting in a material impact and thus should be reported pursuant to Item 8.01 but not Item 1.05.

Rather than producing the promised uniformity and comparability, Item 1.05 has fragmented disclosure, diluted the informational value of each Form 8-K, created interpretive uncertainty about its requirements, and inundated investors with immaterial cybersecurity disclosures made simply to avoid second-guessing by the Commission. This is antithetic to the Commission's overarching goal to protect and inform investors. As stated by Commissioner Pierce earlier this year, the Commission should not mandate disclosure of information when "the direct and indirect costs (borne by investors) of producing it outweigh the benefits to investors of consuming it."[45]

D. The Premature Public Disclosure Mandate Has Been Weaponized by Threat Actors and Increases Legal Exposure

As our petition documented, threat actors have leveraged Item 1.05 as an extortion tool, threatening to report victims to the Commission if they do not pay ransom.[46] In addition, publicly disclosing ongoing incidents is a gift for other threat actors looking to capitalize on an unresolved vulnerability or a registrant's already strained cyber defenses. As Commissioners Peirce and Uyeda have cautioned, the Commission "needs to start treating companies subject to cyberattacks as victims of a crime, rather than perpetrators of one."[47] The Commission should not maintain a disclosure

[44] 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.

[45] Hester M. Peirce, U.S. Sec. & Exch. Comm'n, The Art and Science of Materiality, Remarks at SEC Speaks (Mar. 19, 2026), https://www.sec.gov/newsroom/speeches-statements/peirce-remarks-sec-speaks-031926.

[46] Petition for Rulemaking at 6.

[47] Hester M. Peirce & Mark T. Uyeda, Statement Regarding Administrative Proceedings Against SolarWinds Customers, U.S. Sec. & Exch. Comm'n (Oct. 22, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224.

requirement that criminal actors can use as a coercive instrument to harm companies and their investors.

At the same time, Item 1.05 forces registrants to "lock in" public statements about the scope, impact, and remediation status of an incident at a point when facts are incomplete and evolving, increasing the risk that premature filings may be used by plaintiffs' attorneys in securities class actions or by insurers to deny coverage. Because Item 1.05 disclosures are filed, not furnished, they carry potential liability under Sections 11 and 12 of the Securities Act, including strict liability under Section 11, and Sections 10(b) and 18 of the Exchange Act, and are fertile ground for securities class-action complaints. The result is a disclosure requirement that simultaneously encourages premature, speculative disclosure and penalizes companies for inevitable inaccuracies, undermining both effective incident response and the provision of decision-useful information to investors.

E. Returning to the Pre-Existing, Principles-Based Framework Would Better Serve Investors

Rescinding Item 1.05 and, as discussed above, Item 106 would not leave investors unprotected. Registrants would continue to evaluate and appropriately disclose information on material cybersecurity risks and incidents under the existing framework, which includes Items 101, 103, 105, 303, and 407 of Regulation S-K and the Commission's 2011 and 2018 guidance. In the absence of Item 1.05, registrants could instead use Item 8.01 of Form 8-K to disclose both material cybersecurity incidents and other incidents that a registrant believes relevant to investors. Regulation FD would continue to ensure that material nonpublic information, including material cybersecurity incidents, is disclosed broadly (and not selectively) to the public.

Rescission of Item 1.05 would accomplish a rebalancing of incentives. Companies would be better able to prioritize incident containment, remediation, and coordination with law enforcement and critical-infrastructure authorities in the early days of an event and then provide more accurate and contextualized disclosure once the materiality analysis is complete. Investors would receive fewer but more meaningful reports grounded in a stable factual record rather than inferences drawn under duress. A return to the pre-existing principles-based disclosure framework would better align the timing and content of disclosure with the realities of cybersecurity risk management, ensuring that public reporting reflects informed judgment rather than compelled immediacy.

IV. If Not Rescinded, Item 1.05 and Item 106 Disclosure Should Be Explicitly Entitled to the Safe Harbor Under Section 27A of the Securities Act and Section 21E of the Exchange Act

If Form 8-K, Item 1.05 or Item 106 of Regulation S-K are not rescinded, to protect registrants from liability under the federal securities laws, including Sections 11 and 12 of the Securities Act and Sections 10(b) and 18 of the Exchange Act, for disclosures made pursuant to such requirements, the Commission should explicitly state that forward-looking statements regarding the scope, impact, and remediation of cybersecurity incidents are entitled to the safe harbor for forward-looking statements under Section 27A of the Securities Act and Section 21E of the Exchange Act. The Commission should further clarify that this safe harbor applies equally to corresponding disclosures made by foreign private issuers, including disclosures furnished under Form 6-K or included in Form 20-F, to ensure parity in the

treatment of substantively equivalent cybersecurity disclosures across issuer types. Although the safe harbor applies generally to forward-looking statements, explicit confirmation that it applies to all such cybersecurity disclosures would reduce uncertainty for registrants and better align the liability framework with the inherently evolving nature of cybersecurity incidents.

V. Recommendations

In light of the foregoing, we respectfully recommend that, as part of its comprehensive review of Regulation S-K, the Commission:

1. Rescind Item 106 (and the corresponding Item 16K of Form 20-F) in its entirety, given that cybersecurity risks do not justify a departure from the Commission's principles-based disclosure regime applicable to other risks, and the rule's prescriptive requirements compel disclosure of sensitive operational details that could undermine the efficacy of a registrant's cybersecurity processes.

2. If Item 106 is not rescinded, amend Item 106 (and Item 16K of Form 20-F) to:

   - narrow and align the definition of "cybersecurity incident" to the impact-based standards used in the prudential banking agencies' Computer-Security Incident Notification Rule and narrow and clarify the definition of "information systems"; and
   - streamline the required disclosures to refocus on (i) how registrants integrate cybersecurity risk into enterprise risk management and strategy, and (ii) how the board of directors oversees those risks rather than inventorying specific processes.

3. Rescind Form 8-K, Item 1.05 (and the corresponding Form 6-K provision) and revert to the longstanding principles-based approach for incident disclosure under which material cybersecurity incidents can be appropriately disclosed, through existing current and periodic reporting pathways such as Form 8-K, Item 8.01.

4. If Item 1.05 and Item 106 (and the corresponding Form 6-K and Form 20-F reporting provisions) are not rescinded, provide explicit safe harbor protection under Section 27A of the Securities Act and Section 21E of the Exchange Act for cybersecurity disclosures.

We are committed to working with you to develop a balanced cyber disclosure regime that provides investors with decision-useful information while still acknowledging the operational challenges confronting public companies in the wake of a cyber incident. If you have any questions or would like to discuss these comments further, please reach out to John W. Carlson at jcarlson@aba.com, Patrick Warren at Patrick.warren@bpi.com, Todd Klessman at tklessman@sifma.org, Anjelica Dortch at anjelica.dortch@icba.org, 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/ Patrick Warren
Patrick Warren
Senior Vice President, Assistant General Counsel
Bank Policy Institute

/s/ Todd Klessman
Todd Klessman
Managing Director, Financial Services Cyber & Technology
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

cc: Benjamin R. Pedersen, Partner
Paul M. Rodel, Partner
Debevoise & Plimpton LLP