



October 2, 2026

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

Re: Comment on Reforming Regulation S-K (File No. CLL-15)—Cybersecurity Disclosures

CTIA¹ appreciates the opportunity to submit these comments to the U.S. Securities and Exchange Commission (“SEC” or “Commission”) in response to Chairman Atkins’ request for comment on reforming Regulation S-K.² We welcome the Chairman’s focus on “amend[ing] Regulation S-K, with the goal of revising the requirements to focus on eliciting disclosure of material information and avoid compelling the disclosure of immaterial information.”³ With this letter, we urge the SEC to prioritize reform of its cybersecurity disclosure requirements under Regulation S-K, Item 106,⁴ as well as its related cyber incident disclosure requirements⁵ on Form 8-K, Item 1.05, as part of this effort.

The wireless industry is a leader in cybersecurity, cyber risk management, industry-based security and resilience initiatives, and consumer education. The wireless industry prioritizes and has in depth experience with cybersecurity, as well as cyber incident response, reporting, and information sharing. CTIA works closely with federal agencies and policy makers to develop sound cybersecurity frameworks and prioritizes cybersecurity regulatory harmonization. Consistent with the wireless industry’s commitment to cybersecurity, this letter adds to the already strong support in the record encouraging the SEC to significantly reconsider its cybersecurity disclosures to promote broader, critical efforts to harmonize duplicative cybersecurity reporting requirements, which will ultimately enhance the state of cybersecurity.

¹ CTIA–The Wireless Association® (“CTIA”) (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association’s members include wireless providers, device manufacturers, and suppliers, as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. CTIA represents a broad diversity of stakeholders, and the specific positions outlined in these comments may not reflect the views of all individual members. The association also coordinates the industry’s voluntary best practices and hosts educational events that promote the wireless industry. CTIA was founded in 1984 and is based in Washington, D.C.

² Chairman Paul S. Atkins, *Statement on Reforming Regulation S-K*, SEC (Jan. 13, 2026), <https://www.sec.gov/newsroom/speeches-statements/atkins-statement-reforming-regulation-s-k-011326>.

³ *Id.*

⁴ Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51942–43 (Aug. 4, 2023) (codified at 17 C.F.R. § 229.106) (“Rule”).

⁵ Rule at 51945 (codified at 17 C.F.R. § 249.308).



I. THE SEC SHOULD RECONSIDER ITS APPROACH TO CYBERSECURITY DISCLOSURES.

A. The SEC Should Rescind Its Cybersecurity Disclosure Requirements Under Item 106 of Regulation S-K.

The rigid criteria that the SEC has established for the Item 106 cybersecurity disclosures compel companies to reveal sensitive details on cybersecurity risk management, strategy, and governance practices and impose significant resource requirements on companies. Importantly, the risks and burdens of these disclosures are not counterbalanced by meaningful benefits for investors.

First, disclosures on risk management and strategy offer threat actors insights they can leverage to identify vulnerabilities and navigate around internal protections and third-party oversight mechanisms. These disclosures risk eroding a company's cybersecurity posture by revealing operational details. *Second*, these disclosures also require companies to spend significant time on compliance, preparing the overly detailed disclosures to the detriment of using those resources for security operations. *Third*, the proscriptive requirements in the disclosures require the same details from companies in different sectors, with different levels of cybersecurity risk and different risk management practices. This hamstrings a company into making disclosures that may be ill-tailored for the company's unique cybersecurity program. *Fourth*, overly granular cybersecurity disclosures result in companies providing details on security controls and procedures that are far beyond what a reasonable investor needs to understand material risks to the company and base an investment decision, effectively burying investors in immaterial detail.⁶

In short, Item 106 fails to illicit materiality-centered information about cybersecurity risks and risk management⁷ and it raises serious operational and policy concerns. Accordingly, it should be rescinded as part of the Chairman's deregulatory effort.

B. The SEC Should Rescind the Requirement to Disclose Cybersecurity Incidents Under Item 1.05 of Form 8-K.

The Commission's related requirement to report cybersecurity incidents under Form 8-K, Item 1.05, Material Cyber Incidents,⁸ has similar critical issues as the cybersecurity disclosures under Item 106, with additional detrimental impacts. Specifically, under the current Rule, companies are pressured to report on Form 8-K incidents within four business days of determining an incident is material. Under this approach, companies who are victims of cyber incidents may have to divert resources away from responding to an incident to determine whether reporting has been triggered on a timeline that is short with little flexibility. This overly rigid cybersecurity incident disclosure requirement results in myriad

⁶ Comments of American Bankers Association, et al., File No. CLL-15, at 2 (filed Apr. 10, 2026) ("ABA Regulation S-K Comments").

⁷ *Id.*

⁸ Form 8-K, Item 1.05(a), 17 C.F.R. § 249.308 (2026).



unintended consequences, including increasing compliance burdens and costs, pressuring companies to make premature disclosures in the face of concerns over potential enforcement, providing information that threat actors take advantage of, and creating confusion for companies seeking to comply—all while potentially exposing investors to premature or potentially misleading disclosures.

First, the Item 1.05 disclosure is very costly because materiality determinations regarding cyber incidents have to be assessed constantly, which typically requires assistance from outside counsel and external incident response teams.

Second, under the current approach, companies are pressured to make materiality decisions quickly or risk potential enforcement action testing the timing of those decisions, which can create situations where incidents are disclosed that are not actually material and can lead to less accurate or relevant information being disclosed. As a consequence, this does not provide adequate time for investigations into cybersecurity incidents, which, as CTIA has explained to the SEC, may require months.⁹ The SEC’s emphasis on the need for timely incident information overlooks the possibility that rushed disclosure will lead to less accurate or relevant incident information.¹⁰ Disclosure of incidents before all the information is available and a sufficient investigation has occurred makes it harder to draw accurate conclusions.¹¹ Thus, premature disclosure under the SEC’s Rule can harm a victim company and result in investors receiving incorrect information.

Third, for incidents where a victim company may still be triaging the incident, premature disclosures can undermine cybersecurity and tip off threat actors.¹² As CTIA explained in its earlier comments to the SEC, “[r]e-victimization of companies after a cybersecurity incident is a real threat, and publicly confirming a breach or releasing information about incidents serves as an invitation to malicious actors and opportunists.”¹³ Multiple commenters in the original rulemaking expressed concerns over premature disclosure of an incident prior to remediation, which can set up the victim company for further attacks.¹⁴ In short, the SEC’s near-to-real-time disclosure requirement places victim companies in jeopardy if a cyber incident remains ongoing by alerting the threat actor of detection and other nefarious actors of a company’s vulnerabilities.

Relatedly, it is critical that victim companies are not required to disclose information that could

⁹ Comments of CTIA, File No. S7-09-22, at 12 (filed May 9, 2022) (“CTIA Cyber Disclosures Comments”) (“[A] material incident may require months of analysis before a victim can confidently address the types of information that the SEC would have them make public within four days.”).

¹⁰ *Id.* at 13.

¹¹ *Id.*

¹² ABA Regulation S-K Comments at 10, 12.

¹³ CTIA Cyber Disclosures Comments at 17; *see* ABA Regulation S-K Comments at 12–13.

¹⁴ Comments of Securities Industry and Financial Markets Association, File No. S7-09-22, at 4 (May 9, 2022); Comments of Society for Corporate Governance, File No. S7-09-22, at 4 (filed May 9, 2022); Comments of Information Technology Industry Council, File No. S7-09-22, at 3 (filed May 9, 2022); and Comments of BPI, et al., File No. S7-09-22, at 10 (filed May 9, 2022).



impede law enforcement investigations. Premature incident disclosure can interrupt law enforcement campaigns against threat actors and necessary preparatory measures to secure victim infrastructure. The Federal Bureau of Investigation (“FBI”) recognizes the sensitivity of cyber compromises, including in the context of collaborating with victim companies. This respect for victim confidentiality and protection of sensitive data related to an incident is explicit in the FBI’s Cyber Strategy (2026).¹⁵ Even prior to the strategy, the FBI has delayed announcements related to compromises until after companies have had time to remediate security issues.¹⁶

Under the Item 1.05 disclosure requirement, a registrant may delay disclosure of a material cybersecurity incident only if the Attorney General (“AG”) determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of that determination in writing.¹⁷ This national security or law enforcement delay is far too narrow to accommodate a delay for many companies undertaking coordinated mitigations or investigations with the FBI. Few companies have or would qualify for the limited exception requiring an AG determination that a disclosure would pose a substantial risk to national security or public safety.

Further, the inflexible SEC approach does not accommodate coordination of public statements concerning an incident with security agencies, such as the FBI, “to ensure that harmful or sensitive information is not needlessly disclosed.”¹⁸ DOJ and FBI frequently delay public statements about cybersecurity threats and threat actors until after victim infrastructure is secured or threat actors are expelled,¹⁹ but inflexible rules do not allow for this strategic pattern of disclosure.

Fourth, confusion and practical challenges have been widespread following the adoption of the SEC’s cybersecurity incident disclosure requirement. Indeed, in May 2024, the SEC Division of Corporation Finance issued a clarification regarding mandatory reporting under Item 1.05 and voluntary reporting under other items, acknowledging the complexity of the framework and noting that “it could be confusing for investors if companies disclose either immaterial cybersecurity incidents or incidents for which a materiality determination has not yet been made under Item 1.05.”²⁰ Still, following the release of this guidance, the requirements and guidance around reporting remains complex and ripe for confusion. For example, some companies continue to file disclosures under Item 1.05 without the

¹⁵ See *Federal Bureau of Investigation Cyber Strategy*, FBI (Sept. 9, 2026).

¹⁶ Press Release, Department of Justice, *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant* (Dec. 19, 2023) (“DOJ ALPHV/Blackcat Ransomware Variant Press Release”); Press Release, Department of Justice, *U.S. government disrupts botnet People’s Republic of China used to conceal hacking of critical infrastructure* (Jan. 31, 2024) (“DOJ CI Hacking Press Release”).

¹⁷ Form 8-K, Item 1.05(c), 17 C.F.R. § 249.308 (2025).

¹⁸ CTIA Cyber Disclosures Comments at 15.

¹⁹ With the ALPHV/Blackcat ransomware, the DOJ delayed the announcement of the ransomware group until after the FBI shared the decryption key with victims allowing them to restore their systems. See DOJ ALPHV/Blackcat Ransomware Variant Press Release.

²⁰ Erik Gerding, *Disclosure of Cybersecurity Incidents Determined to Be Material and Other Cybersecurity Incidents*, SEC (May 21, 2024).



requisite materiality determination, reflecting this ongoing confusion.²¹ Similarly, specific aspects of the SEC’s approach—*e.g.*, the distinction between “material” and “material impact”—continue to contribute to uncertainty regarding the appropriate Form 8-K item.²² Given that these challenges have not been fully resolved, this further supports rescinding the requirement to disclose cybersecurity incidents under Item 1.05 of Form 8-K.

For all of these reasons, the SEC should rescind mandatory reporting under Item 1.05 and return to the historical practice of reporting cyber incidents voluntarily on Form 8-K. This would accommodate the disclosure of both material cybersecurity incidents and other incidents that a company believes relevant to investors.²³ This approach allows adequate flexibility for companies to voluntarily report an incident “after the incident has been contained.”²⁴

II. TAKING A MORE FLEXIBLE APPROACH TO CYBERSECURITY DISCLOSURES IS CONSISTENT WITH CRITICAL HARMONIZATION GOALS.

Congress, the Department of Homeland Security, and other agencies have routinely promoted flexible policy approaches to addressing cybersecurity that balance the benefits of disclosure against cybersecurity, national security, and other considerations that promote confidentiality. For example, in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCA”), Congress established confidential treatment for cyber incident reports.²⁵ Other federal²⁶ and state laws²⁷ recognize the benefits of confidential treatment and careful disclosure of cybersecurity incidents to accommodate ongoing investigations or to not disrupt response actions, such as botnet takedowns.²⁸ In the context of coordinated vulnerability disclosures, both the government and the private sector recognize the need to balance the benefits of releasing information to the public with the risks of premature disclosure²⁹ before mitigations or other protections are available.³⁰

Unfortunately, as discussed above, the SEC’s current approach to cybersecurity disclosures

²¹ Avi Gesser et al., *Cybersecurity Incident Disclosure: Form 8-K Tracker (Two-Year Update)*, Debevoise & Plimpton LLP (May 21, 2026).

²² See generally Letter from Thomas J. Kim, Partner, Gibson, Dunn & Crutcher LLP on behalf of David R. McAtee II, Senior Executive Vice President and General Counsel, AT&T Inc., to Division of Corporation Finance, SEC, File No 001-08610 (filed July 31, 2024), <https://www.sec.gov/Archives/edgar/data/732717/000119312524190323/filename1.htm>.

²³ ABA Regulation S-K Comments at 12.

²⁴ Comments of National Association of Manufacturers, File No. CLL-15, at 7 (filed Apr. 13, 2026).

²⁵ See 6 U.S.C. § 681e(b).

²⁶ See 48 C.F.R. § 252.204-7012(h); Memorandum from Ha Nguyen McNeill, Acting Administrator, TSA, on Renewal of the Security Directive (SD) 1580-21-01 series: *Enhancing Rail Cybersecurity* (Jan. 9, 2026).

²⁷ See, *e.g.*, N.Y. Comp. Codes R. & Regs. tit. 23, § 500.18.

²⁸ NIST SP 800-150, Guide to Cyber Threat Information Sharing, NIST, at 4 (Oct. 2016); see also DOJ CI Hacking Press Release.

²⁹ See, *e.g.*, NIST SP 800-216, Recommendations for Federal Vulnerability Disclosure Guidelines, NIST, at 18 (May 2023).

³⁰ See ISO/IEC 29147:2018, Information technology—Security techniques—Vulnerability disclosure.



deviates from this widely accepted standard, imposing prescriptive requirements regarding strategy, governance, and incident disclosure.³¹ Accordingly, the SEC should rescind Regulation S-K, Item 106 and the Form 8-K, Item 1.05 cybersecurity reporting requirement. Specifically with respect to incident reporting, the SEC should follow other federal cybersecurity regimes that take a flexible approach to allow for confidentiality surrounding cybersecurity incidents. This would allow victim companies adequate time to respond to active threats and provide investors with complete information.

Reconsidering the current cybersecurity disclosure requirements will promote broader efforts towards harmonization. In a July 22, 2026 assessment of federal cybersecurity reporting requirements, the U.S. Government Accountability Office (“GAO”) found that overlapping requirements are widespread, identifying 48 cyber incident reporting requirements on the federal level that required private entities to report within various timeframes³² and that reporting obligations are duplicative.³³ In addition to federal requirements, states, including New York, also require cybersecurity incident reporting.³⁴ Currently, the Commission’s incident disclosure regime adds a further layer to an already fragmented federal and state landscape.

The negative impacts of this type of fragmentation are real. The U.S. Chamber of Commerce and McCrary Institute for Cyber and Critical Infrastructure Security recently warned that duplicative cyber incident reporting requirements can force companies to respond to multiple agencies, pulling resources away from containing the incident and securing systems.³⁵ These findings are consistent with prior assessments of duplicative cyber incident reporting requirements and the impacts of this regulation on the private sector.³⁶

To address these issues, Congress and the executive branch are engaged in concerted work to harmonize cyber incident reporting. For example, Congress deliberately prioritized cyber incident reporting harmonization in CIRCIA. In the 119th and 118th Congresses, the Senate considered legislation to establish a framework for reciprocal compliance mechanisms for cybersecurity requirements and a pilot project on harmonization.³⁷ Congress has held multiple hearings on cybersecurity harmonization.³⁸ Additionally, in 2023, members of Congress in the House and Senate

³¹ Rule at 51945.

³² GAO, *Cybersecurity Regulations: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements*, GAO-26-108606, at 5 (July 22, 2026).

³³ *Id.* at 3–6.

³⁴ N.Y. Comp. Codes R. & Regs. tit. 23, § 500.17(a)(1).

³⁵ McCrary Institute for Cyber and Critical Infrastructure Security & U.S. Chamber of Commerce, *From Fragmentation to Coordination: Operationalizing U.S. Cyber Incident Reporting*, at 11 (Aug. 31, 2026).

³⁶ Office of the National Cyber Director, *Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information*, The White House, at 5 (June 2024).

³⁷ See Streamlining Federal Cybersecurity Regulations Act of 2025, S. 1875, 119th Cong. (2025).

³⁸ *Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime: Before the Subcomm. on Cybersecurity and Infrastructure Prot. of the H. Comm on Homeland Sec.*, 119th Cong. 1 (2025); *Cybersecurity Regulation Harmonization: Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 115th Cong. 1



introduced a Congressional Review Act resolution to overturn the SEC cybersecurity risk management, strategy, governance, and incident disclosure Rule.³⁹ Similarly, the White House issued the National Cyber Strategy for America (“Strategy”) on March 6, 2026, which prioritizes the promotion of common sense regulation as a primary goal of the Administration.⁴⁰ Specifically, the Strategy calls for “streamlin[ing] cyber regulations to reduce compliance burdens, address liability, and better align regulators and industry globally.”⁴¹ The Strategy makes clear that piling on cybersecurity incident reporting requirements on U.S. companies is out of step with not only the Administration’s cybersecurity policy priorities, but also its overall deregulatory agenda.⁴²

The SEC’s efforts to amend its cybersecurity disclosure requirements can contribute to those efforts. Specifically, rescinding Regulation S-K, Item 106 and Form 8-K, Item 1.05 will alleviate the burdens of disclosures under the current rigid SEC Rule and provide greater flexibility for harmonizing in the direction of Congress’ and the Administration’s goals.

III. CONCLUSION

CTIA appreciates this opportunity to comment on regulatory reforms at the SEC. As part of the Chairman’s focus on reforming Regulation S-K, CTIA joins others in the record urging the SEC to rescind (1) the prescriptive cybersecurity disclosures under Regulation S-K, Item 106, which require companies to disclose sensitive operational details on cybersecurity risk management, strategy, and governance practices, while inundating investors with immaterial information, and (2) the related cyber incident disclosure requirement under Form 8-K, Item 1.05, which pressures companies to make premature disclosures, which can undermine—not enhance—cybersecurity. Instead, the SEC should take a more flexible approach that will balance providing meaningful information to investors with important operational, policy, and technical considerations. Ultimately, a new approach to cybersecurity disclosures will enable better cybersecurity outcomes and align the SEC with Congress’ and the Administration’s harmonization and deregulation goals.

Sincerely,

Avonne S. Bell

/s/

Avonne S. Bell
Director, Connected Life

(2017); *Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization: Before the S. Comm on Homeland Sec. & Governmental Affairs*, 118th Cong. 2 (2024).

³⁹ H.R.J. Res. 100, 118th Cong. (2023).

⁴⁰ *President Trump’s Cyber Strategy for America*, The White House (Mar. 6, 2026).

⁴¹ *Id.* at 5.

⁴² See Exec. Order 14192, 90 Fed. Reg. 9065 (Jan. 31, 2025).



Umair Javed
Senior Vice President and General Counsel

Kurt Schaubach
Senior Vice President and Chief Technology
Officer

John A. Marinho
Vice President, Cybersecurity & Technology

Afeite Dadjia
Director, Cybersecurity