May 9, 2022

The Honorable Gary Gensler, Chairman
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

**VIA EMAIL** (rule-comments@sec.gov)

RE: File Number S7-09-22, Comments of the National Retail Federation in Response to the SEC's Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Chairman Gensler:

The National Retail Federation (NRF) respectfully submits this comment upon the Securities and Exchange Commission's (SEC or Commission) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed Rule (cybersecurity rule or proposal).

NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants, and internet retailers from the United States and more than 45 other countries. The purpose of NRF is to advocate for the economic and policy interests of retailers. NRF regularly convenes hundreds of retail brands to discuss data privacy and cybersecurity matters. Cybersecurity issues are increasingly important to retailers as more retail business is conducted online each year. A secure cyberspace is crucial to the functioning of our members operating online and in traditional store fronts.

NRF is committed to the important issue of ensuring retailers—both online and in person—are safe and secure in their online functions for the protection of their customers, employees, and investors. Although we acknowledge the substantial interest in protecting companies and their customers from cybersecurity threats, we believe the proposal suffers from several legal and policy flaws and should not be finalized in its current structure.

- *The Commission lacks legal authority to finalize the cybersecurity rule.* The statutory context of the SEC's enabling legislation demonstrates that the SEC's power to issue disclosure rules is limited to specific types of information closely related to the disclosing company's value and financial condition. The cybersecurity rule seeks to require disclosure of information beyond these limits and thus exceeds the SEC's statutory authority. The proposal, if finalized, also raises serious constitutional questions regarding the separation of powers.

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

- *The cybersecurity rule is inconsistent with the Securities and the Exchange Acts' objectives and would be arbitrary and capricious if finalized.* Each aspect of the proposal suffers from practical challenges that undermine any advantages to investors from the required disclosures. The incident disclosure rule will make companies more vulnerable to further attacks, disrupt incident response measures, and it lacks clear guidelines of what is material in the cybersecurity incident context. The policy disclosure rule will highlight company vulnerabilities to both cyber criminals and competition. The governance disclosure rule is unnecessary to protect investors and micromanages company cybersecurity governance measures, which goes beyond the Commission's expertise.

- *The cybersecurity rule is not cost effective.* The costs of complying with the cybersecurity rule, which will include renegotiating contracts with third-party IT professionals and increased auditing costs, among others, cannot be justified—especially when the proposal acknowledges that it is unable to quantify the potential benefit of the rule to investors. Less burdensome alternatives to the proposal, like maintaining the status quo under the SEC's 2018 guidance pertaining to cybersecurity disclosures, would inform investors of cybersecurity risks that may affect the value of a security in a more cost-effective manner.

## I. The Commission Lacks Legal Authority to Finalize the Cybersecurity Rule.

***Statutory Authority***: The SEC's rulemaking authority is limited to topics for which Congress has expressly delegated rulemaking authority.[1] Generally speaking, the SEC is charged with protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation.[2] Its authority does not extend to all aspects of registrant company operations, and the proposal oversteps the Commission's delegated authority by seeking to regulate private companies' cybersecurity disclosures and policies.

The proposal's only discussion of the SEC's statutory basis for delving into cybersecurity is a single sentence asserting that the SEC proposes the cybersecurity rule "under the authority set forth in Sections 7 and 19(a) of the Securities Act and Sections 3(b), 12, 13, 14, 15, and 23(a) of the Exchange Act."[3] This is insufficient for two reasons: First, this conclusory statement fails to provide stakeholders a meaningful opportunity to comment upon the authorities on which the Commission relies for the proposal. Second, although Congress may have given the SEC

[1] *New York Stock Exch. LLC v. SEC*, 962 F.3d 541, 554 (D.C. Cir. 2020); *see also Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986) ("[A]n agency literally has no power to act . . . unless and until Congress confers power upon it.").

[2] The Exchange Act authorizes the SEC "to facilitate the establishment of a national market system for securities" and "having due regard for the public interest, the protection of investors, and the maintenance of fair and orderly markets, to use its authority" to achieve this goal. 15 U.S.C. § 78k-1(a)(2).

[3] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590, 16,618 (proposed March 23, 2022) (to be codified at 17 C.F.R. pts. 229, 232, 239, 240, 249).

rulemaking authority necessary to implement these provisions of the statutes, it is not clear how or why the proposal furthers those provisions. And the SEC's apparent interpretation of its authority surpasses that granted to it by Congress because the Commission fails to read the cited sections of the Securities and Exchange Acts in their statutory context.

The proposal deprives NRF a meaningful opportunity to comment upon the legality of the rule because it does not specify which provisions of the relevant statutes the proposal would carry out (other than a passing citation, without elaboration, to over 70 pages of statutory text).[4] The opportunity for public comment on proposed regulations must be a "meaningful opportunity."[5] Further explanation of the actual statutory authority upon which the SEC intends to rely, with an explanation for why the proposal is necessary or appropriate to achieve the statute's goals, is necessary for the SEC to receive effective comments and ensure the proposal is set to withstand inevitable future legal challenges.

In any event, although not specifically discussed in the proposal, NRF assumes the SEC is purporting to act under the provisions granting the Commission rulemaking authority in Sections 7(a)(1) and 19(a) of the Securities Act and Sections 12(b)(1), 13(a), and 23(a) of the Exchange Act.[6] These provisions give the SEC specific authority to require certain financial disclosures and the general authority to make rules "necessary or appropriate" to carry out the provisions of the Securities Act and Exchange Act, but this rulemaking authority is not boundless.

Section 19(a) of the Securities Act empowers the SEC to "make . . . rules and regulations as may be necessary to carry out the provisions of [the Securities Act]."[7] Likewise, Section 23(a) of the Exchange Act empowers the SEC "to make such rules and regulations as may be necessary or appropriate to implement the provisions of [the Exchange Act]."[8] However, these grants of authority cannot be read in isolation but must be read to only enable rulemaking, as the statutes make plain, to carry out another specific "provision" of the Act. As the United States Court of Appeals for the District of Columbia Circuit recently explained, these general provisions do not "empower the agency to pursue rulemaking that is not otherwise authorized[.]"[9] In other words,

---

[4] *Id.*

[5] *Rural Cellular Ass'n v. FCC*, 588 F.3d 1095, 1101 (D.C. Cir. 2009).

[6] 15 U.S.C. §§ 77g(a)(1), 77s(a), 78l(b)(1), 78m(a), 78w(a).

[7] *Id.* § 77s(a).

[8] *Id.* § 78w(a)(1).

[9] In *New York Stock Exchange LLC*, the Court analyzed, and ultimately vacated, a SEC rule promulgated under the Commission's general rulemaking authority in Section 23(a) of the Exchange Act. *See* 962 F.3d at 556. The Court relied on *Michigan v. EPA*, where the Supreme Court made clear that the mere reference to "necessary" or "appropriate" in a statutory provision authorizing an agency to engage in rulemaking does not afford the agency authority to adopt regulations as it sees fit with respect to all matters covered by the agency's authorizing statute. *Id.; see also Michigan v. EPA*, 576 U.S. 743, 751 (2015) ("EPA strayed far beyond th[e] bounds [of reasonable

these general grants of authority, alone, are insufficient to provide the SEC with legal authority to finalize the proposal.

Moreover, the rulemaking provision's statutory context belies any assertion that they confer broad authority beyond what is necessary or appropriate to implement some other specific provision of the Acts. It is a "fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme."[10] The statutory context of the Securities Act and the Exchange Act demonstrates that the SEC's power to issue disclosure rules is limited to specific types of information closely related to the disclosing company's value and financial condition.

The language after the general rulemaking provision in Section 19(a) of the Securities Act is instructive in this regard. After the grant of general rulemaking authority, the Act lists "examples" of authority the SEC has under the provision. These include generating forms, detailing items included on a balance statement, and dictating the methods to be followed in the preparation of accounts.[11] These examples show that this general rulemaking power is not all-encompassing, but that Congress meant to empower the SEC to determine details necessary to fulfill specific directives in the Securities Act and Exchange Act.

Because the general rulemaking provisions alone are insufficient to empower the SEC to finalize the proposal, the SEC must specify which provision of the Securities Act and Exchange Act it is acting under. The proposal does make a passing citation to other statutory provisions that reference rulemaking authority in its one sentence explanation of statutory authority. Specifically, Section 7(a)(1) of the Securities Act and Sections 12(b)(1) and 13(a) of the Exchange Act give the Commission authority to impose some disclosure obligations. These specific directives, however, when read in context, likewise fall short of giving the SEC the authority to finalize the proposal.

First, Section 7(a)(1) of the Securities Act serves a very specific purpose that the proposal does not further.[12] Entitled "Information Required in Registration Statement," Section 7 provides that a registration statement for a security must "be accompanied by the documents, specified in Schedule A."[13] Schedule A, included in the Securities Act at 15 U.S.C. § 77AA, is a detailed list of 32 required documents that reveal information about the identity of the actors involved and the financial status of a company. Schedule A requires, for example, disclosure of the names and addresses of the directors, the amount of securities of the issuer held by the directors (and other

---

interpretation] when it read [an "appropriate and necessary" provision] to mean that it could ignore cost when deciding whether to regulate power plants.").

[10] *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000) (quoting *Davis v. Michigan Dept. of Treasury*, 489 U.S. 803, 809 (1989)).

[11] 15 U.S.C. § 77s(a).

[12] *Id.* § 77g(a)(1).

[13] *Id.*

key persons), and the amount of the funded debt outstanding.[14] These disclosures are meant to reveal less apparent interests, liabilities, and financial information about the company to potential investors. The House report preceding the Securities Act explained that items in Schedule A "are items indispensable to any accurate judgment upon the value of a security . . . [t]he type of information to be disclosed is of a character comparable to that demanded by competent bankers from their borrowers[.]"[15] Schedule A does not mention cybersecurity or any other similarly specific aspect of a company's operations. Rather, as the SEC has acknowledged, the items in Schedule A "are largely financial in nature and were intended to help investors assess a security's value."[16]

Section 7(a)(1) of the Securities Act contains two caveats. First, the SEC may promulgate a rule excluding some Schedule A information from a required disclosure if it concludes the information is not necessary for adequate disclosure to investors in particular classes of issuers.[17] Second, the specific rulemaking provision comes in: the SEC may adopt rules to require a registration statement to include other information or documents as "necessary or appropriate in the public interest or for the protection of investors."[18] Thus, when this rulemaking provision is read in context, it becomes clear that Congress gave the Commission the ability to require the disclosure of additional Schedule A-type documents, which are largely financial in nature. Although the SEC may exclude and supplement certain Schedule A information, the Commission should not read the rulemaking provision in Section 7(a)(1) to allow it to require broad disclosures on any topic, like cybersecurity incidents and policies.

Second, Section 12(b)(1) of the Exchange Act, which explains the necessary information to include in an application for registering a security, also contains a specific rulemaking provision. Section 12(b)(1) provides that an application shall contain "information, in such detail as to the issuer [and affiliated entities and persons] as the Commission may by rules and regulations require, as necessary or appropriate in the public interest or for the protection of investors, *in respect to the following* [categories of information]."[19] Section 12(b)(1)(A)-(L) then lists 12 specific categories of information, including the nature of the business, the terms of outstanding securities, descriptions of directors, officers, and major shareholders, material contracts, balance sheets, profit and loss statements, and other financial statements. These categories, of course, do not include

[14] *Id.* §§ 77AA(4), (7), (12).

[15] H.R Rep. No. 73-85, 73rd Cong., 1st Sess., 1933.

[16] SEC, Concept Release, *Business and Financial Disclosure Required by Regulation S-K*, 81 Fed. Reg. 23,916, 23,921 (April 22, 2016).

[17] 15 U.S.C. § 77g(a)(1) ("[T]he Commission may by rules or regulations provide that such information or document need not be included in respect of any class of issuers or securities if it finds that the requirement of such information or document is inapplicable to such class and that disclosure fully adequate for protection of investors is otherwise required to be included within the registration statement.").

[18] *Id.*

[19] *Id.* § 78l(b)(1) (emphasis added).

cybersecurity information. When Section 12(b)(1)'s rulemaking provision is read in the limited sense of creating rules directly related to the prescribed categories of information, it is clear that the Commission does not have authority under this provision to promulgate cybersecurity disclosure requirements.

Third, Section 13(a) of the Exchange Act contains a rulemaking provision, which, like Section 12(a), is limited to rules requiring the disclosure of financial information when read in context. Section 13(a) provides:

> Every issuer of a [registered security] shall file with the Commission, in accordance with such rules and regulations as the Commission may prescribe as necessary or appropriate for the proper protection of investors and to insure fair dealing in the security--
>
> > (1) such information . . . the Commission shall require to keep reasonably current the information [supplied to register securities under Section 12 of the Exchange Act]
> >
> > (2) such annual reports . . . certified if required . . . by independent public accountants, and such quarterly reports . . . as the Commission may prescribe.[20]

The statutory language allowing the SEC to issue rules requiring annual and quarterly reports has no explicit subject-matter restriction in Section 13(a)(2). But the provision is limited when read together with Section 13(b)(1). Section 13(b)(1) demonstrates that the rulemaking power granted to the SEC regarding requiring annual and quarterly reports is limited to subjects directly related to balance sheets, earnings statements, and related items indicative of financial health, not cybersecurity protocols. Specifically, Section 13(b)(1) provides:

> The Commission may prescribe, *in regard to reports made pursuant to this chapter*, the form or forms in which the required information shall be set forth, the items or details to be shown in the balance sheet and the earnings statement, and the methods to be followed in the preparation of reports, in the appraisal or valuation of assets and liabilities, in the determination of depreciation and depletion, in the differentiation of recurring and nonrecurring income, in the differentiation of investment and operating income, and in the preparation, where the Commission deems it necessary or desirable, of separate and/or consolidated balance sheets or income accounts of any person directly or indirectly controlling or controlled by the issuer, or any person under direct or indirect common control with the issuer[.][21]

---

[20] *Id.* § 78m(a)(1)-(2).

[21] *Id.* § 78m(b)(1) (emphasis added).

This limited reading of Section 13(a)(2) makes sense. Section 13(a)(2) gives the SEC authority to require annual reports to be certified by independent public accountants. It would be quite unusual for cybersecurity disclosures required by the proposal (or similar non-financial information) to benefit from certification by public accountants who have no expertise in cybersecurity. This limited reading is likewise confirmed by the House report for the Exchange Act, which emphasizes that annual and quarterly company reports would provide financial and accounting information "to give some assurance that reports will not hide the true condition of the company."[22]

When the rulemaking provisions in the Securities Act and Exchange Act are read in context, as they must, the provisions are circumscribed more than the proposal seems to acknowledge—they are best read to empower the SEC to require disclosures of specific financial information to give investors a true picture of the securities on the market.

Moreover, when Congress desires that the SEC require public companies to disclose information beyond the clearly financial information authorized by the Securities Act and Exchange Act, Congress specifically authorizes the Commission to prescribe such rules in further statutory enactments. For example, Congress has used statutory authorizations to require disclosures on corporate responsibility, corporate governance, and selected aspects of executive compensation.[23] Indeed, Congress frequently updates the securities laws, and yet it tellingly has not charged the Commission with requiring cybersecurity disclosures like those in the proposal.[24]

But Congress has not been silent in the area of cybersecurity. Acknowledging that cybersecurity is an issue of paramount concern to the safety and security of our country, Congress has repeatedly legislated to combat this ever-growing national security and economic threat and has empowered federal agencies other than the SEC to serve that important purpose.[25] Just this

---

[22] H.R. Rep. No. 73-1383, at 11–13, 24 (1934).

[23] *See* 81 Fed. Reg. at 23,922.

[24] *See, e.g.*, Securities Investor Protection Act of 1970, 15 U.S.C. §§ 78aaa et seq. (1970); Private Securities Litigation Reform Act of 1995, 15 U.S.C. §§ 77-78 (1995); Securities Litigation Uniform Standards Act of 1998, Pub. L. No. 105-353, 112 Stat. 3227 (1998) (codified as amended in scattered sections of 15 U.S.C.); Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002) (codified as amended in 15 U.S.C. §§ 7201-7266 and scattered sections of 18 U.S.C. and 28 U.S.C.); Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.); Jumpstart Our Business Startups Act (JOBS Act), Pub. L. No. 112-106, 126 Stat. 306 (2012) (codified as amended in scattered sections of 15 U.S.C.).

[25] *See, e.g.*, Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022) § 2242(b)(1) (directing the Cybersecurity and Infrastructure Security Agency to promulgate regulations to implement the Act's reporting obligations for covered entities); Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C. § 652 (creating the Cybersecurity and Infrastructure Security Agency); Cybersecurity Act of 2015, 6 U.S.C. §§ 1504(a)(4) (directing the Attorney General and the Secretary of the Department of Homeland Security to develop guidance to promote sharing of cyber threat indicators with Federal entities); Federal Information Security

past legislative session, over 157 cybersecurity bills were introduced, and one significant cybersecurity reporting act was passed, which empowered the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations to implement the Act's cybersecurity reporting mandates.[26] Congress also annually combats cybercrime through the appropriations process.[27] Congress has charged other agencies (like CISA, DHS, the FBI, and other components of the federal law enforcement community) to combat this important problem, and the SEC should not usurp the undelegated role of maintaining cyber safety in America. Cybersecurity is certainly an area of growing importance to companies across the world. "Regardless of how serious the problem" is, the Commission cannot "exercise its authority 'in a manner that is inconsistent with the administrative structure that Congress enacted into law.'"[28]

***Separation of Powers***: If the SEC's authority is not limited to requiring public disclosures of financially related information, as demonstrated by the text and context of the Securities and Exchange Acts, the proposal faces a separate set of legal failings. The major questions doctrine and the non-delegation doctrine are both principles that "protect the separation of powers and ensure that any new laws governing the lives of Americans are subject to the robust democratic processes the Constitution demands."[29]

Under the major questions doctrine, the courts "expect Congress to speak clearly if it wishes to assign to an executive agency decisions of vast economic and political significance."[30] In compliance with this doctrine, Congress has spoken clearly when it previously authorized the Commission to require disclosures related to specific public policy concerns, such as "conflict minerals."[31] As previously noted, if Congress meant for the SEC to broadly regulate public companies' cybersecurity policy and disclosures, it would have clearly authorized it to do so with the requisite specificity.

---

Modernization Act of 2014, 44 U.S.C. §§ 3551, 3554 (codifying information security requirements for the federal government to be administered by the Office of Management and Budget and the Department of Homeland Security)..

[26] Georgia Wood, *Cybersecurity Legislation in the 117th Congress*, Center for Strategic & International Studies (Dec. 6, 2021), https://www.csis.org/blogs/strategic-technologies-blog/cybersecurity-legislation-117th-congress; Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022).

[27] For example, the Consolidated Appropriations Act of 2022 expands CISA's budget by more than 28 percent relative to the budget enacted for fiscal year 2021 (and more than $460 million over the administration's request for fiscal year 2022). *See* Consolidated Appropriations Act, 2022, H.R. 2471, 117th Cong. (2022).

[28] *Ragsdale v. Wolverine World Wide, Inc.*, 535 U.S. 81, 91 (2002) (quoting *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125 (2000)).

[29] *NFIB v. OSHA*, 142 S. Ct. 661, 668–69 (2022) (Gorsuch, J., concurring).

[30] *Id.* at 655.

[31] Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), 15 U.S.C. § 78m(p) (2010); *see also* Business and Financial Disclosure Required by Regulation S-K, 81 Fed. Reg. at 23,969-70 (explaining that Congress mandated that the Commission adopt rules regarding registrants' use of "conflict minerals.").

If the Securities Act and Exchange Act were as broad as the SEC seemingly interprets them to be, and somehow delegates limitless authority for the SEC to require public disclosures on *any* topic it deems in the "public interest" or as "protecting investors," then the proposal may raise serious concerns about whether the Acts would violate the non-delegation doctrine.[32]

## II. The Cybersecurity Rule Is Inconsistent with the Commission's Statutory Objectives and Would be Arbitrary and Capricious if Finalized.

Even if the SEC had the authority to finalize the proposal, it should choose not to because it is inconsistent with the objectives of the Securities Act and Exchange Act. Each aspect of the proposal—the incident disclosures, policy disclosures, and governance disclosures—suffers from practical challenges which undermine any advantages to investors from disclosure. Accordingly, the proposal does not serve the SEC's mission to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. Rather, the proposal imposes unnecessary costs and risks upon disclosing companies while wading into an area better regulated by Congress and the agencies specifically tasked with combatting cybersecurity threats. The SEC has not "articulate[d] a satisfactory explanation" for proposing the rule.[33] As such, it would be arbitrary and capricious if finalized.

***Incident Disclosure***: The proposal's requirement to report incidents four days after the incident becomes "material" (even if still ongoing) could disrupt incident response measures, including ongoing mitigation efforts, law enforcement outreach, and the voluntary sharing of threat information with other companies via Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). Any law or regulation requiring the disclosure of a cybersecurity breach that is still ongoing should have protections in place for the disclosing company. For example, some state laws require disclosure of a cybersecurity incident in an even shorter time frame than the proposal, but those required disclosures are of a different character. State security breach disclosure laws require disclosures to be made directly to the affected persons and entities, rather than to the public.[34] These state disclosure laws also typically have other safeguards in place for the disclosing company like law enforcement exemptions that delay a company's disclosure obligation.[35] Similarly, Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act, which requires covered entities to report certain cyber

[32] *See NFIB*, 142 S. Ct. at 669 (Gorsuch, J., concurring).

[33] *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (explaining that an agency must explain that there is a "rational connection between the facts found and the choice made" (quoting *Burlington Truck Lines v. United States*, 371 U.S. 156, 168 (1962)).

[34] All 50 states have some version of a security breach notification law which requires businesses to notify individuals of a security breach of information involving personally identifiable information. *See, e.g.*, O.C.G.A. 10-1-912 (requiring breached third parties to notify the relevant data owners or licensees within 24 hours of the discovery of a breach if personal information was, or is reasonably believed to have been, acquired by an unauthorized person).

[35] *Id.* (noting that the required notification may be delayed for law enforcement purposes).

incidents to CISA within 72 hours of the incident.[36] However, the Act cloaks covered entities who disclose cybersecurity incidents to the agency with a variety of liability (and other) protections to incentivize fair and accurate reporting.[37] Unlike similar state and federal laws, the proposed cybersecurity rule would require companies to *publicly* disclose a breach, with no exemptions or protections, in a four-day time frame, which may deprive the company of the chance to fully understand the nature and impacts of the attack or remedy the invasion before disclosing. This time frame may also lead to disclosures that are incomplete or later found to be inaccurate, given the inherently ambiguous nature of many potential cyber incidents. Requiring this disclosure before the full containment and remediation of the incident publicizes to other bad actors that the company has at least one exploitable vulnerability and may allow cybercriminals to further victimize the company—the disclosure could even prompt cybercriminals to begin hunting for the breached data. This could increase the ultimate harm to the company, owners of the stolen data, and accordingly increase the harm to investors.

The four-day timeline will also shift important resources away from what should be companies' highest priorities in response to potential cyber incidents: containing and remediating vulnerabilities, and mitigating and preventing any damages or loss. As part of incident response, many companies also appropriately prioritize engagement with law enforcement to support investigative activities, and the sharing of threat information on a voluntary basis (including with ISACs and ISAOs) to prevent future incidents. Instead, this four-day timeline will compel companies to devote a large share of their cyber teams' resources toward compliance with reporting requirements and making recurrent determinations about the potential materiality of incidents. Requiring companies to report incidents within four days will unreasonably divert attention away from crucial response measures and could impair or chill companies' existing efforts to engagement with law enforcement and share cyber threat information. To the extent reporting to the SEC would be appropriate at all, it should be within a reasonable time *after* the incident has been resolved.

Further, without clear guidelines of what is material in this specific context, the SEC will expose the regulated community to arbitrary enforcement and liability. The concept of materiality refers to information that a reasonable investor would find important in making an investment decision. If a cyber-attack were so extensive that it would impact the financial health of a company or the fruitfulness of an investment, existing requirements would likely already require disclosure. As such, the proposed requirement suggests that the commission anticipates some other metric. And without the Commission explaining what that metric is and under what authority the Commission imposes it, the proposal would subject the regulated community to arbitrary enforcement. The lack of clear guidance as to what constitutes a material cybersecurity incident also presents a due process problem. A regulation that does not "give ordinary people fair notice

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

[37] *See* H.R. 2471 § 2245(a)–(c).

of the conduct it punishes" violates an essential requirement of due process.[38] If people "of common intelligence must necessarily guess at [a regulation's] meaning," like they would here, it will be deemed unconstitutionally vague.[39]

***Cybersecurity Risk Management and Strategy***: The proposal's requirement to disclose policies and procedures to manage cybersecurity risks may highlight company vulnerabilities that could be exploited by cyber criminals or competition. The proposal would require registrants to describe their "policies and procedures . . . for the identification and management of risks from cybersecurity threats."[40] It is undoubtably important for companies to maintain such policies and procedures. Yet it is equally important for them to remain nimble and able to address quickly emerging threats and trends. The level of detail required by the proposal would allow cybercriminals to search for and exploit vulnerabilities in those policies and procedures and prevent the degree of flexibility companies need to change practices and procedures as threats emerge. It also may expose proprietary or confidential processes to competition. As written, the proposal has not grappled with how the potential benefits, if any, from the proposal would outweigh these threats.

This section of the SEC's proposal also includes a problematic requirement for companies to disclose information with respect to their use of assessors, consultants, auditors and other third-parties to support cyber risk assessment. The SEC's proposal seems to imply that this information would contribute to a meaningful assessment of a company's cybersecurity risk management. There is no clear basis to assert that the use of such third parties is a determinant of improved cybersecurity risk management, and many of NRF's member companies have developed internal cybersecurity risk management capabilities that obviate the need for the extensive use of such third-parties.

***Governance Disclosure***: The SEC has not explained why a detailed list of governance-related cybersecurity disclosures is needed for the protection of investors. The regulation would require, among other things, the disclosure of: (1) a board member's cybersecurity expertise, (2) whether the company has a chief information security officer, their relevant expertise, and where they fit in the organizational chart, and (3) granular information about the interactions of management and the board of directors on cybersecurity, including the frequency with which the various actors discuss the topic.[41] This level of detail in governance-related information is unprecedented in SEC regulation, is inflexible in its approach, and is simply not needed for investors to make sound investment decisions. As Commissioner Pierce explains, this laundry list of requirements, in a way, dictates the Commission's expectations for how a company's governance should be

[38] *Johnson v. United States*, 576 U.S. 591, 595 (2015); *Boyce Motor Lines, Inc. v. United States*, 342 U.S. 337, 338-39 (1952) (considering a vagueness challenge to an administrative regulation).

[39] *Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926).

[40] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. at 16,619.

[41] *Id.* at 16,600.

structured to withstand cybersecurity threats.[42] This area is beyond the Commission's expertise. "While the integration of cybersecurity expertise into corporate decision-making likely is a prudent business decision . . . whether, how, and when to do so should be left to business—not SEC—judgment."[43]

For instance, the proposal's requirement that companies disclose the cybersecurity expertise of board members (which implicitly preferences such expertise in board members) may be unsound business judgment for most registrants. Board members are not directly implementing cybersecurity policy—especially in industries such as retail, in which cyber security is not the core business—and it is unclear why there should be an expectation that all public companies search for and elect board members with cybersecurity expertise. Of course, board members should be aware of technology and general cybersecurity risks to help make decisions and manage corporate risk on behalf of the company. But board members are not directly implementing cybersecurity policy or responding to cybersecurity incidents, which makes specific training and expertise in cybersecurity response measures unnecessary. In addition, as a practical matter, because cybersecurity best practices and technical capabilities are constantly evolving, it is unclear how, for example, a decades-old degree or certification in cybersecurity would be especially helpful in managing the risks cybersecurity poses to public companies today.

## III. The Commission Should Fully Consider the Economic Costs of the Cybersecurity Rule Before Finalizing.

The proposal underestimates the costs associated with complying with the rule. For instance, managing relationships with third-party IT professionals to comply with reporting obligations is costly and will require companies to renegotiate contracts and relationships with third party service providers in order to further support reporting obligations. Specifically, the proposal will expand the degree of third-party audit costs that registrants must incur to assure the accuracy of the reported information. Many NRF members already spend millions of dollars on average per year auditing SEC disclosures. Each added requirement will substantially increase those efforts.

What is more, it is unclear that the proposal will inure benefits that could even begin to justify its costs. The SEC has a "statutory obligation to determine as best it can the economic implications of the [proposal.]"[44] As the proposal notes, the Commission has been "unable to quantify the potential benefit to investors and other market participants" from the increased disclosure requirements in the proposal. Although the Commission may not need to quantify all potential

---

[42] *See* Commissioner Hester M. Peirce, *Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal by Commissioner Peirce*, SEC.GOV (March 9, 2022), https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922 ("Such precise disclosure requirements look more like a list of expectations about what issuers' cybersecurity programs should look like and how they should operate.").

[43] *Id.*

[44] *Chamber of Com. of the United States of America v. SEC*, 412 F.3d 133, 143 (D.C. Cir. 2005).

benefits, it must undertake a reasonable assessment of them. And it cannot do so without supporting predictive judgements, quantifying costs where it can, and relying upon empirical data.

Instead of doing so, the proposal merely speculates about the benefits. For example, the proposal suggests that investors would benefit from more informed disclosure, but it does not say how or cite to any studies that specifically explain why investors would benefit from the newly required information or how the lack of that information has harmed them. It speculates that "delayed or incomplete reporting of cybersecurity incidents and risks *could* lead to mispricing of securities" without identifying any incidents, let alone widespread incidents, where it has.[45] It suggests that registrants "*could*" benefit from more uniform disclosures, but concedes that it is unable to assess those benefits.[46] The proposal suggests that the cybersecurity rule "could have positive effects on market efficiency," but fails to assess whether and how it actually will. Absent more information that would reasonably suggest investors would benefit from the proposal's requirements, the Commission simply fails to meet its obligation to assess the proposal's economic implications.

Lastly, alternatives to the proposal would achieve the SEC's desired objective in a more cost-effective manner. For example, the Commission could simply require registrants to disclose whether they have cybersecurity measures in place and more generally disclose material risks and how they would be mitigated, rather than detailing a laundry list of policy and governance information to be disclosed. This alternative to the proposal would just as effectively inform investors of the true value of their securities—with a much lower cost.

Further, maintaining the SEC's current cybersecurity incident reporting regime is more cost effective than finalizing the proposal. The status quo of cybersecurity disclosures under the SEC's current guidance best balances the competing interests at play. Under the SEC's current guidance, from its 2018 Interpretive Release, companies already should "timely" disclose information in periodic reports about material cybersecurity incidents to investors.[47] This guidance provides companies with needed discretion to ascertain the relevant facts to be disclosed and acknowledges that "some material facts may not be available at the time of the initial disclosure," that a company "may require time to discern the implications of a cybersecurity incident," and that "ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident."[48] The 2018 Interpretive Release strikes the right balance between keeping investors informed of cybersecurity incidents that may affect a security's value and leaving companies with needed control over their policies, procedures, and incident response. In the absence of evidence

[45] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. at 16,608.

[46] *Id.* at 16,612.

[47] SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 1, 12 (Feb. 26, 2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf (explaining that companies should provide timely and ongoing information in periodic reports (Form 10-Q, Form 10-K, and Form 20-F) about material cybersecurity risks and incidents that trigger disclosure obligations).

[48] *Id.*

that the current reporting regime has deprived investors of material information on a widespread basis, the proposed changes, with their attendant costs, cannot be justified.

For the above stated reasons, NRF respectfully requests that the Commission decline to finalize the proposal in its current structure. We would be pleased to discuss further amendments to the proposal that would advance cybersecurity goals within the limits of the Commission's authority.

Sincerely,

Stephanie A. Martz
Chief Administrative Officer and General Counsel
National Retail Federation