United States Senate
COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510–6250

May 9, 2022

VIA EMAIL (rule-comment@sec.gov)

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

RE: SEC Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, File No. S7-09-22

Dear Ms. Countryman:

I am writing to you as the Ranking Member of the United States Senate Committee on Homeland Security and Governmental Affairs regarding the Securities and Exchange Commission (SEC) proposed rule that would require registrants to disclose material cyber incidents publicly.[1] I am concerned the detailed public disclosures this rule proposes risks providing cybercriminals with information they could exploit to damage national cybersecurity, impair law enforcement investigations, and frustrate Government responses to cyberattacks.

The proposed rule acknowledges it "could potentially increase the vulnerability of registrants and the risk of future attacks."[2] Despite recognition of this and other concerns, the proposed rule deems the potential value of public cyber incident disclosures as outweighing the security risks. This risk contradicts Congress's legislative intent with the enactment of the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, a bill I co-authored. That law seeks to enhance the visibility of the United States Government into cyberattacks against critical infrastructure. Through increased information sharing, the Government will be better positioned to coordinate its response to cyberattacks and warn potential victims. At the same time, the law has appropriate liability, privacy, and use protections for the information reported to the Government, in part to ensure that victims are not made more vulnerable by their disclosures to the Government.

This letter discusses the issues surrounding the proposed rule's lack of an exception for an ongoing law enforcement investigation, public disclosure of ongoing cyber incidents, and public disclosure of company cybersecurity plans and procedures. It also documents Congress's intent that the *Cyber Incident Reporting for Critical Infrastructure Act* be the primary

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 63 (Mar. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[2] *Id.* at 62.

mechanism for companies to report cyber incidents. The SEC should work closely with the National Cyber Director, the Department of Homeland Security, and industry stakeholders to deconflict existing reporting requirements and ensure the proposed rule does not require companies to disclose information that would put their security at risk.

LAW ENFORCEMENT INVESTIGATION EXEMPTION

The SEC's proposed rule does not allow companies to delay disclosure because of ongoing law enforcement investigations or related Governmental actions. The proposed rule correctly notes "that a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents."[3] Premature public disclosure can also hinder a variety of important Government functions including deterrence and recovery actions, attribution, broader remediation, and sharing of threat and vulnerability information with other potential targets. Nevertheless, the SEC maintains "that the importance of timely disclosure of cybersecurity incidents for investors would justify not providing a reporting delay."[4] I disagree.

The SEC's proposal not to provide a reporting delay conflicts with state breach notification laws, which do provide for delayed reporting in the case of an ongoing law enforcement investigation.[5] The proposed rule expressly acknowledges this saying, "there is a possibility a registrant would be required to disclose [an] incident on Form 8-K even though it could delay incident reporting under a particular state law."[6] Even the SEC itself is entitled to delay reporting a breach of its own systems to affected individuals when necessary to avoid impairing law enforcement or other Governmental actions. Under OMB guidance, the SEC may delay notification to individuals potentially impacted by a breach if the Attorney General, head of an element of the Intelligence Community, or the Secretary of Homeland Security determines "the notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions."[7] In effect, the proposed rule prioritizes prompt public disclosure of information regarding material cybersecurity incidents over law enforcement and national security risks.

In enacting the *Cyber Incident Reporting for Critical Infrastructure Act*, Congress concluded the opposite. The law makes congressional intent clear—incident reporting requirements should not impair law enforcement investigations and other important security-related work. For example, while "communication[s], document[s], material[s], or other record[s], created for the sole purpose of preparing, drafting, or submitting" an incident report

[3] *Id.* at 25.
[4] *Id.*
[5] *Id.*; *see also, e.g.*, *Security Breach Notification Laws*, NAT. CONF. ST. LEGISLATURES (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[6] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 26 (Mar. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[7] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-17-12, PREPARING FOR AND RESPONDING TO A BREACH OF PERSONALLY IDENTIFIABLE INFORMATION 31 (2017).

cannot be received in evidence, law enforcement can use the reported information to investigate cyber incidents.[8]

When considering the legislation, Congress noted if the FBI is "provided information from reports under the process outlined in the statute, [it] may, as appropriate, use information contained in the reports and derived from them" for a range of investigatory activities.[9] This is consistent with the statute which states incident reports can be used for "the purpose preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident" reported under the law.[10] This allows law enforcement agencies to disrupt and deter hostile cyber actors, while maintaining the law's "goal of encouraging entities to disclose cyber incidents" to the Federal Government.[11]

In a dissenting statement on the proposed SEC rule, Commissioner Hester Peirce expressed similar concerns regarding law enforcement investigations. Ms. Peirce said her "primary concern with the proposed incident reporting requirements is that we are unduly dismissive of the need to cooperate with, and sometimes defer to, our partners across the Federal Government and state government."[12] On law enforcement investigation exemptions specifically, she correctly noted if such a delay would increase the likelihood of holding cybercriminals accountable, then the SEC "should consider whether temporary relief from our disclosure requirements would best protect investors."[13] Such an exemption would be consistent not only with existing state breach notification laws, but also Congress's intent, reflected in the recent enactment of the *Cyber Incident Reporting for Critical Infrastructure Act*.

ONGOING CYBER INCIDENT DISCLOSURE

The proposed rule also requires companies to disclose ongoing cyber incidents. In particular, the rule "would not provide for a reporting delay when there is an ongoing *internal* . . . investigation related to the cybersecurity incident."[14] The rule justifies this saying, "while an ongoing investigation might affect the specifics in the registrant's disclosure, 'an ongoing internal investigation or external investigation—which often can be lengthy—would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.'"[15]

Forcing companies to disclose cyber incidents publicly and before they have a complete understanding of those incidents, mitigate the damage and vulnerabilities, and contain malicious

[8] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Division Y−Cyber Incident Reporting for Critical Infrastructure Act (2022).
[9] 168 CONG. REC. S 1,149−50 (daily ed. Mar. 14, 2022).
[10] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Division Y−Cyber Incident Reporting for Critical Infrastructure Act (2022).
[11] 168 CONG. REC. S 1,149−50 (daily ed. Mar. 14, 2022).
[12] Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal (Mar. 9, 2022), https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922.
[13] *Id.*
[14] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 25 (Mar. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11038.pdf (emphasis added).
[15] *Id.* (quoting Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 12 (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf).

actors presents significant security risks. Nefarious cyber actors—both criminal organizations and nation state actors—are adept at collecting intelligence on their victims and leveraging that information in their attacks and ransomware negotiations.[16] Requiring the disclosure of information on ongoing incidents may allow hackers to identify the "crown jewels" or most valuable information held by an organization amongst vast quantities of data. It could also help attackers improve targeting, gain additional access, effect further damage, and, in the case of ransomware, demand larger ransoms. Public disclosure of an ongoing incident also puts companies at risk of follow-on or copycat attacks by other malicious actors. For example, with the recent disclosure of vulnerabilities in Microsoft Exchange server and Apache log4j, attackers were quick to exploit systems when patches were unavailable or not fully implemented.[17] If the registrant is required to disclose an incident before completing remediation of the vulnerability by which an attacker gained access, other opportunistic attackers may identify and exploit the vulnerability to perpetrate further cyberattacks against the registrant. Similarly, if the method of attack is novel involving a "zero day" vulnerability for which no patch exists yet, other organizations which use the vulnerable system or software will also be exposed to attack.[18] This is important for all cyber incident victims but presents grave national security risks as it relates to critical infrastructure and Federal partners.

Protecting this sensitive incident information was a priority for Congress during its recent consideration of the *Cyber Incident Reporting for Critical Infrastructure Act*. Senate debate on the legislation reiterated this, saying the bill sought to ensure "that entities are encouraged to and feel protected in disclosing cyber incidents."[19] To achieve this, the statute limits the further sharing of and appropriate uses for reported information and establishes confidentiality and anonymization protections for sharing that information with relevant stakeholders.[20] Congress devised these protections to avoid placing entities at risk by complying with the reporting requirements in the statute. The SEC's requirement to disclose ongoing incidents could place registrants at greater risk, imperil the reporting information the Federal Government will receive under the now enacted *Cyber Incident Reporting for Critical Infrastructure Act*, and complicate efforts to prevent future incidents.

I also note that disclosure of an ongoing incident risks contradicting the SEC's stated goal of reducing mispricing of securities because such information is preliminary and thus potentially inaccurate.[21] If initial information on an incident subsequently proves inaccurate, premature

---

[16] *E.g.*, STAFF OF S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, 117TH CONG., AMERICA'S DATA HELD HOSTAGE: CASE STUDIES IN RANSOMWARE ATTACKS ON AMERICAN COMPANIES 11 (2022) ("some ransomware attackers will even seek out cyber insurance policy information to aid in their negotiations with victims").
[17] Tom Burt, *New nation-state cyberattacks*, MICROSOFT (Mar. 2, 2021), https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/; *Alert (AA21-356A): Mitigating Log4Shell and Other Log4j-Related Vulnerabilities*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Dec. 23, 2021), https://www.cisa.gov/uscert/ncas/alerts/aa21-356a.
[18] U.S. DEP'T OF COMMERCE & U.S. DEP'T OF HOMELAND SEC., ASSESSMENT OF THE CRITICAL SUPPLY CHAINS SUPPORTING THE U.S. INFORMATION AND COMMUNICATIONS TECHNOLOGY INDUSTRY 43 (2022).
[19] 168 CONG. REC. S 1,149−50 (daily ed. Mar. 14, 2022).
[20] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Division Y−Cyber Incident Reporting for Critical Infrastructure Act (2022).
[21] *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Jen Easterly, Director, CISA)

public disclosure risks providing investors with inaccurate information that could result in mispricing and ill-informed investor decisions, assuming investors consider that information in making investment decisions.

CYBER PLAN AND PROCEDURE DISCLOSURE

The proposed rule would also require companies to disclose policies and procedures used "to identify and manage cybersecurity risks and threats."[22] Among other things, this includes policies to address cyber threats like intellectual property theft, fraud, extortion, and violation of privacy laws.[23] The proposed rule would also require companies to disclose detailed descriptions of their cybersecurity risk assessment programs, including whether companies retain third-party providers as part of that plan.[24] The level of specificity the proposed rule requires for these disclosures could implicitly identify a company's vulnerabilities so attackers could select the weakest targets and formulate a more effective attack strategy. This increased risk outweighs whatever limited value disclosing these procedures to investors might have. The SEC should consider these unintended risks and adopt a more restrained approach for achieving its goal to better inform investors of a company's approach to cyber risk management.

Congress confronted a similar issue when drafting the *Cyber Incident Reporting for Critical Infrastructure Act*. During the drafting process, Congress sought to enable "a coordinated, informed U.S. response to cyber attacks" and "warn other critical infrastructure operators similarly situated."[25] Nevertheless, Congress was careful to only require the reporting of information that would directly contribute to a more coordinated United States response to cyber incidents. During a committee hearing on the legislation, I acknowledged this saying, "there is a balance between getting information quickly, letting victims respond to an attack without imposing onerous requirements on them and getting accurate information. We understand that balance."[26] This measured approach allowed Congress "to be sure [it was] actually doing what [it] intend[ed] to do, which is to help both the private sector and governmental agencies deal with cyberattacks."[27]

CONGRESS INTENDED THAT THE CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT BE THE PRIMARY MECHANISM FOR COMPANIES TO REPORT CYBER INCIDENTS

The Commission cites "growing concern that material cyber incidents are underreported . . ." as the impetus for the proposed rule, referencing mid-2021 comments by the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland

("We don't want to be flooded with reports saying, we detected something, we're not sure whether there's actual impact or not. I think we need to make sure that there's determined impact").

[22] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 37 (Mar. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[23] *Id.*

[24] *Id.* at 37−38.

[25] 168 CONG. REC. S 930−32 (daily ed. Mar. 2, 2022) (statement of Sen. Portman).

[26] *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 117th Cong. (2021) (statement of Sen. Rob Portman).

[27] *Id.*

Security (DHS) and Congress, including one of the authors of the *Cyber Incident Reporting for Critical Infrastructure Act*.[28] Congress addressed this deficiency by enacting the *Cyber Incident Reporting for Critical Infrastructure Act* which first passed the Senate on March 1, 2022—eight days before the SEC released its proposed rule to address the same concerns.[29]

Congress intended that the *Cyber Incident Reporting for Critical Infrastructure Act* be the primary means for reporting of cyber incidents to the Federal Government, that such reporting be through CISA, and that the required rule occupy the space regarding cyber incident reporting. The legislation's requirement that DHS create a cyber incident reporting council "to coordinate, deconflict, and harmonize Federal incident reporting requirements" serves as evidence of this intent.[30]

Congress considered expanding the legislation's incident reporting requirements beyond critical infrastructure and whether to make such information public. Ultimately, Congress determined cyber incident reports should be submitted to CISA, by critical infrastructure, and remain confidential. This determination was made in part after considering some of the same issues discussed above, and concluding that reports from our most vital industry sectors would best position the Federal Government to respond to and mitigate attacks.[31]

CONCLUSION

SEC's proposed rule would increase cyber risks for many companies, could impair national security as it relates to critical infrastructure and Federal partners, and contradicts Congress's intent to harmonize cyber incident reporting requirements and provide appropriate protections for cyber incident information reported to the Government. I encourage SEC to reconsider or revise substantially the proposed rule.

Sincerely,

Rob Portman
Ranking Member

[28] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 20 (Mar. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[29] S. 3600, 117th Cong. (2022) (passed Senate on Mar. 1, 2022).
[30] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Division Y−Cyber Incident Reporting for Critical Infrastructure Act (2022).
[31] 168 CONG. REC. S 1,149−50 (daily ed. Mar. 14, 2022).