

Congress of the United States
House of Representatives
Washington, DC 20515-3202

September 1, 2023

The Honorable Gary Gensler
Chair
U.S. Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Dear Chair Gensler:

We write expressing serious concerns over the Securities and Exchange Commission's (SEC) new Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure final rules. While the SEC's intent may be to standardize disclosures regarding cybersecurity governance and incident reporting by public companies, these new expansive disclosure requirements for public companies will do just the opposite by duplicating and confusing existing cyber incident reporting requirements. Further, the new rules compromise the confidentiality of a company's cybersecurity program, thus harming investors instead of protecting them as the rules purport to do.

On July 26, the SEC adopted the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure final rules. The new disclosure rules will require registrants to publicly disclose on the new Item 1.05 of Form 8-K any cybersecurity incident they determine to be material; to describe the material aspects of the incident's nature, scope, and timing; and to describe its material impact or reasonably likely material impact on the registrant. The registrant will be required to make this disclosure four business days after it determines that a cybersecurity incident is material, unless the Attorney General determines that disclosure would threaten national security or public safety. Additionally, the rules add Regulation S-K Item 106, which requires a registrant to describe its processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats and to describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.¹

The SEC's cybersecurity disclosures are in direct conflict with the congressionally-mandated Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which is currently being implemented by the Cybersecurity and Infrastructure Security Agency (CISA). Signed into law in March 2022, CIRCIA requires CISA to develop and issue regulations requiring covered entities to report to CISA any covered cyber incidents within 72 hours from the time the entity reasonably believes the incident occurred – a rulemaking that is currently being developed. CIRCIA also establishes the Cyber Incident Reporting Council (Council) at the Department of Homeland Security (DHS) to coordinate, deconflict, and harmonize federal incident reporting requirements.² By giving CISA and DHS these directives, Congress solidified its intent that CISA is the lead Federal agency for cybersecurity and should be the primary intake point for cyber incident reports. While CIRCIA aims to equip CISA with incident information to offer technical assistance, mitigate impacts for other organizations, and ultimately identify trends to protect the homeland, the SEC rules aim to increase transparency for investors. It is unfathomable that the SEC is moving forward with its public disclosure requirements, which will only increase cybersecurity risk, without a congressional mandate and in direct contradiction to public law that is intended to secure the homeland.

¹ <https://www.sec.gov/news/press-release/2023-139>

² <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia#:~:text=Cyber%20Incident%20Reporting%20Requirements%3A%20CIRCIA,reasonably%20believes%20the%20incident%20occurred.>

Congress of the United States
House of Representatives
Washington, DC 20515-3202

It is clear that our nation must increase resilience to cyber risk across the board, particularly within our critical infrastructure sectors. However, we must find the right balance between regulatory burden and improving security outcomes. Congress has made it clear that there should not be competing incident reporting requirements. Moving forward, Federal agencies should work to achieve regulatory harmonization, so additional rulemaking does not create duplicative and burdensome regulations.

The passage of CIRCIA proved that cyber regulatory harmonization is a bipartisan priority in Congress, and the Administration itself has emphasized it as well. In the recent National Cybersecurity Strategy and accompanying Implementation Plan, the Administration highlights the importance of harmonizing cyber regulations across the government as well as harmonizing incident reporting requirements, specifically. The former challenge is given to the Office of the National Cyber Director to implement, while the latter is given to the congressionally-created Council. It is clear that these recently issued SEC rules run contrary to both congressional and Administration intent.

Further, while the SEC affirmed that information is material if “there is a substantial likelihood that a reasonable shareholder would consider it important” in making an investment decision, or it would have “significantly altered the ‘total mix’ of information made available,” the SEC also indicated that companies should consider qualitative factors in assessing the material impact of an incident.³ It indicated that harm to a company’s reputation, customer or vendor relationships, or competitiveness, and the possibility of litigation or regulatory investigations or actions, were all potential material impacts on a company. As written, the materiality of an incident can be broadly interpreted, a tactic that the SEC has taken in other rulemakings, and when combined with the requirement that a company must consider what is material to a reasonable investor, the SEC is lowering the bar of what is material.

Greater transparency around cybersecurity risk management, strategy, governance, and material cybersecurity incidents can increase resilience. However, public disclosure of ongoing incidents risks opening registrants up to further attacks. While the SEC makes some changes to the scope of reporting to limit what is reported, publicly reporting even the existence of a material incident before it is remediated would achieve the same effect as disclosing a vulnerability before there is a patch. This would only lead to attackers flocking to exploit the vulnerability for themselves. Additionally, the SEC notes that some companies already disclose material incidents while they are ongoing and that the reporting of such incidents is inconsistent. But, a company voluntarily disclosing an ongoing incident when it feels capable of mitigating any accompanying risk is different than a blanket requirement for reports before a company is capable to fully remediate the risks.

In the end, disclosing an incident too early or disclosing incomplete or inaccurate information may increase exploitation of vulnerabilities, jeopardize investigations, and increase the likelihood of frivolous litigation. This will only harm investors and result in mispriced securities and uninformed market speculation.

Finally, the new rules require new annual report disclosures regarding a company’s cybersecurity policies, procedures, and risk management. Disclosing such information could potentially compromise the confidentiality of a company’s cybersecurity program and reveal details such as the scope and frequency of testing, the nature of third-party systems, and specific remediation activities. The SEC should ensure that these reports do not provide ample information for bad actors to exploit potential vulnerabilities.

³ <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

Congress of the United States

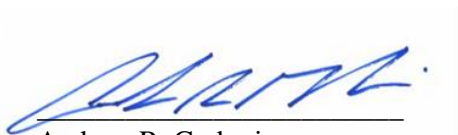
House of Representatives

Washington, DC 20515-3202

Given the potentially harmful consequences of the final rule, we urge the SEC to delay the rule until the SEC works with the Council to determine how the rule interacts with CIRCIA and other Federal prudential regulators' cybersecurity incident reporting requirements. Furthermore, we call on the SEC to conduct a complete internal analysis of how this rule will interact with the SEC's other cybersecurity disclosure proposals before this final rule goes into effect. Failing to do so will only jeopardize companies' confidential reporting strategies and publicly divulge vulnerabilities to our Nation's critical infrastructure.

Thank you for your attention to this matter.

Sincerely,



Andrew R. Garbarino
Member of Congress



Mark E. Green, MD
Member of Congress



Zach Nunn
Member of Congress