May 9, 2022

U.S. Securities and Exchange Commission
Washington, DC 20549

File Number S7-09-22 – Comments on Proposed Rules

The undersigned submits public comments in support of the rules proposed by the U.S. Securities and Exchange Commission ("The Commission") on March 9, 2022, regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies ("the Proposed Rules").

The undersigned are analysts at the Center on Cyber and Technology Innovation (CCTI) at the Foundation for Defense of Democracies (FDD), a nonprofit, nonpartisan 501(c)(3) research institute focusing on foreign policy and national security. CCTI seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. The undersigned submits these comments in their individual capacities. The views expressed herein do not necessarily reflect the views of FDD, its staff, or its advisors.

I. Summary of the Undersigned Position and Issue

By submitting these comments on the Proposed Rules, the undersigned supports the objectives of the Commission to require public companies to (1) report material cybersecurity incidents on Form 8-K; (2) disclose policies and procedures to identify, implement, and oversight of cybersecurity risk management, in addition to updates on previously reported cybersecurity incidents; and (3) present cybersecurity disclosures in Inline eXtensible Business Reporting Language (Inline XBRL).[1]

The Proposed Rules would revise the Commission's 2018 Cybersecurity Guidance[2] by specifying a timeline for companies to notify the Commission of cyber incidents. The Proposed Rules also provide clear guidance on cybersecurity disclosures and governance, motivating companies to better protect their networks, maintain cybersecurity records, and assess risks. Through the Proposed Rules, the Commission can strengthen the resilience and fidelity of American companies by standardizing cyber incident reports, making them publicly accessible, and increasing corporate governance transparency.

We are seeing trends in how corporate cyber hygiene impacts our economy following major cyber incidents, like the SolarWinds hack. Similar to the 2002 Sarbanes-Oxley Act, the Proposed Rules encourage corporate transparency on information available to investors.[3] The investigation led by

[1] U.S. Securities and Exchange Commission, "Public Company Cybersecurity; Proposed Rules," (https://www.sec.gov/files/33-11038-fact-sheet.pdf)
[2] U.S. Securities and Exchange Commission, "SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures," February 21, 2018. (https://www.sec.gov/news/press-release/2018-22)
[3] Tom Fanning, Samantha Ravich, and Suzanne Spaulding, "Why a Sarbanes-Oxley Update Is Needed to Protect Our Financial Sector From Hackers," the Hill, December 28, 2020. (https://thehill.com/blogs/congress-blog/technology/531781-why-a-sarbanes-oxley-update-is-needed-to-protect-our-financial/)

former Commissioner Robert Jackson found that approximately 90 percent of cyber incidents went undisclosed according to 2018 public filings and 97 percent went undisclosed in 2017.[4] We believe that the Commission's Proposed Rules address these issues by emphasizing the role of corporate responsibility in mitigating systemic risks and providing guidance on cyber risk management best practices.

We believe that the Proposed Rules try to achieve two things. First, it attempts to mend the communication breakdown between the United States government and the private sector. Policymakers and corporate executives disagree on policies and procedures for effective cyber risk management. Second, it addresses the problems that arise from the information gap between companies and the public. Transparency into how cyber risk impacts financial operations not only provides a holistic overview of financial performance to investors but also consistent data for the cyber insurance industry to develop accurate risk models.

II. Considerations for the Commission

There are opportunities for improvements to the Proposed Rules. Specifically, the Commission should (1) identify which metrics are required for companies to assess their cyber risk; (2) define cybersecurity incidents that are "material in the aggregate"; and (3) specify the qualifications of board members related to cybersecurity expertise. [5] Overall, the Proposed Rules show a significant effort in encouraging cyber incident reporting and information sharing while creating public pressure on companies to improve their cybersecurity policies and procedures.

a. Metrics

To accurately collect information for practical gap analysis the Proposed Rule should include clear metrics that can capture the company's resilience against potential cyber risks. The key challenge is to consolidate and analyze the collected data to highlight areas for improvement in corporate governance and cyber risk management. The Commission must define what success would look like as companies from various industries develop, improve, and implement cyber risk management policies and procedures required by the Proposed Rules.

In addition, regulatory scrutiny could place heavy operational burdens on companies unevenly. The Commission should consider whether these metrics can reveal an insightful analysis of cyber risk threats that public companies face. For example, cybersecurity incidents that may uniquely impact particular industries may not pose a more significant threat to companies in other sectors.

b. Cybersecurity Incidents That are Material in the Aggregate

While the Proposed Rules include examples of cybersecurity incidents, registrants are left to decide whether the incident should be reported based on the importance of information to the registrant's business operations and networking systems. Thus, the Commission should outline the quantitative

[4] Gabriel T. Rubin, "Many Company Hacks Go Undisclosed to SEC Despite Regulator Efforts." The Wall Street Journal, February 26, 2019. (https://www.wsj.com/articles/many-company-hacks-go-undisclosed-to-sec-despite-regulator-efforts-11551218919?mod=article_inline)

[5] U.S. Securities and Exchange Commission, "Public Company Cybersecurity; Proposed Rules."

and qualitative factors of a cyber incident with a high probability of causing significant harm and loss to business operations. In addition, the Commission should consider whether registrants can obtain and share information to determine the materiality of related incidents when using third-party resources for incident management.

Lastly, the Commission should specify reporting requirements for previously determined immaterial incidents that are material in the aggregate. Currently, the Proposed Rules require "any information"[6] within the registrant's systems, which could include large amounts of data collected from an unidentified period. Thus, clarifying information that registrants will need to share following a cyber incident and outlining policies and procedures for ease in determining immaterial incidents from material ones. Practical reporting requirements would include but are not limited to identifying (1) effective recordkeeping tools; (2) information needed for potential disclosure on material incidents; and (3) ways to provide updates on ongoing incidents.

c. Disclosure of Board's Governance and Expertise

The Commission should consider identifying "audit committee financial expert"[7] similar to the guidelines of the Sarbanes-Oxley Act. The guidelines can provide the registrants with the qualifications and expertise necessary to meet the Proposed Rules' regulatory measures. In addition, the Commission should consider the limited pool of cybersecurity professionals available to meet the appropriate requirements set by the Proposed Rules.

We believe that the Commission's primary intent is to ensure that registrants provide increased transparency to the public and investors through the Proposed Rules. This effort would help preserve the confidence investors place on public companies and allow the public to better evaluate their investment opportunities. The Commission's efforts will encourage companies to take corporate responsibility in mitigating cyber risks as the Proposed Rules act as measures to protect American interests.

The Center on Cyber and Technology Innovation thanks the Commission for the opportunity to submit these public comments. Questions regarding these comments can be addressed to info@fdd.org.

Sincerely,

RADM (Ret.) Mark Montgomery, Senior Director & Jiwon Ma, Program Analyst
The Center on Cyber and Technology Innovation
Foundation for Defense of Democracies
P.O. Box 33249
Washington D.C. 20033

[6] U.S. Securities and Exchange Commission,
"Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Page 41.
https://www.sec.gov/rules/proposed/2022/33-11038.pdf

[7] U.S. Securities and Exchange Commission. 17 CFR Parts 228, 229, and 249. https://www.sec.gov/rules/final/33-8177.htm