Before the
SECURITIES AND EXCHANGE COMMISSION
Washington, DC 20230

In the Matter of	)	
	)	
Cybersecurity Risk Management,	)	
Strategy, Governance, and Incident Disclosure	)	File No. S7-09-22
	)	

COMMENTS OF
USTELECOM—THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] submits these comments in response to the Securities and Exchange Commission ("Commission") proposed rules for disclosures regarding cybersecurity risk management, strategy, and governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.[2]

USTelecom supports the Commission's interest in bringing clarity to providers' duties to reasonably disclose cybersecurity incidents in the interests of investors. We share the goal of ensuring fair disclosure to investors. However, the Commission must balance competing important interests. It must balance the desire to provide prompt public disclosure to assist investors with the important interest in ensuring that disclosures contain useful information rather than being issued too soon, while too much information may still be unknown. Separately,

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives—all providing advanced communications services to both urban and rural markets.

[2] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, File No. S7-09-22 (rel. Mar. 9, 2022) ("Proposed Rules").

the Commission must strike a balance between the interest in disclosure and the benefit that keeping an incident confidential may provide to investigation and resolution of the incident. The Commission should also streamline any rules it may adopt with existing federal and state requirements in this space.

USTelecom's long of history of collaboration with U.S. government partners informs our comments in these proceedings. USTelecom presently chairs the Communications Sector Coordinating Council ("CSCC"), which is among the principal organizations serving as the government's industry partners for developing cybersecurity policies that affect the internet ecosystem.

USTelecom founded, and presently co-leads with the Consumer Technology Association, the Council to Secure the Digital Economy ("CSDE"), a group of fifteen large international ICT companies dedicated to preserving the security of our communications infrastructure and connected digital ecosystem.[3] CSDE is recognized by the U.S. government as a leading industry partnership in coordinating efforts to combat botnets, respond to cyber crises, and promote cybersecurity through development of best practices.

As our leadership in these efforts makes clear, USTelecom fully recognizes the significant cybersecurity challenges facing our nation's infrastructure and broader stakeholder community. USTelecom is committed to finding proactive solutions that help the U.S. government achieve its goals and offers these comments in the spirit of partnership and collaboration.

[3] CSDE, https://csde.org.

I. THE REPORTING WINDOW SHOULD ACCOMMODATE LAW ENFORCEMENT, STATE LAWS, AND COMPANIES' EFFORTS TO PROVIDE ACTIONABLE INFORMATION

The Commission proposes a public reporting window of only four business days.[4] While USTelecom supports a reporting requirement in principle, an inflexible four-business-day disclosure requirement is not appropriate. Providers might not be able to say anything useful in four days and may be able to provide publicly only limited information at that point regarding an evolving situation. Disclosures at that point could cause unnecessary public speculation as to the cause and effect and scope of a given cybersecurity incident. Such speculation could, contrary to the Commission's intent, lead to worse outcomes for investors. Moreover, the negative publicity that may come in the early days of an incident will disproportionately impact companies with more mature cyber programs, who may ultimately be more successful in mitigating the incident.

Any reporting window should also take into account state laws or requests from law enforcement to delay reporting when appropriate to enable law enforcement to conduct investigations of cybersecurity events before they become public. The Commission's proposal would potentially disrupt public-private partnership relationships with law enforcement, which our industry has cultivated over many decades.

Law enforcement efforts are essential to deterring cybercriminals, and doing so ultimately benefits investors across the digital economy. For example, last year, law enforcement disrupted Emotet — referred to as the world's most dangerous malware by Interpol and Europol — with an international takedown operation.[5] Moreover, law enforcement efforts can help companies and investors recover after suffering an attack. For instance, after the Colonial

[4] Proposed Rules at Part II (B) (1).

[5] CSDE, International Botnet and IoT Security Guide (2022), https://csde.org/wp-content/uploads/2022/04/2022-CSDE-International-Botnet-and-IOT-Security-Guide-1.pdf.

Pipeline attack, the Federal Bureau of Investigation ("FBI") was able to successfully claw back a substantial amount of the ransom. A public reporting requirement in the four-day timeframe, as opposed to a more flexible timeframe, could jeopardize such efforts.

We also note the potential conflict between the Commission's proposed rules and the Federal Communications Commission's ("FCC") Customer Network Proprietary Information ("CPNI") rules, which require carriers to report CPNI breaches to the Secret Service and FBI within seven business days, *without* publicly disclosing the breaches for seven days after notifying law enforcement.[6]

II. DETAILED DISCLOSURE OF CYBER RISK MANAGEMENT STRATEGIES CREATES CYBERSECURITY RISKS

The Commission notes that, in 2021, most companies that disclosed a cyber incident did not describe their cyber risk management strategies, while others provided only general information rather than in-depth descriptions.[7] The Commission now proposes Item 106(b) of Regulation S-K to require "more consistent and detailed disclosure regarding their cybersecurity risk management and strategy."[8]

This approach is misguided for two reasons. To begin with, there is an inherent risk in malicious actors having detailed information about cyber risk management strategies. The fact that so many companies declined to disclose more detailed information reflects the reality of this risk.

---

[6] 47 CFR § 64.2011 (b) (1). FCC Chairwoman Rosenworcel has indicated an interest in initiating a proceeding to update these rules. *See* FCC Jan. 12, 2022 News Release, https://www.fcc.gov/document/chair-rosenworcel-circulates-new-data-breach-reporting-requirements. USTelecom urges this Commission and the FCC, along with other federal agencies, to coordinate efforts and align requirements.

[7] Proposed Rules at Part II (D) (1).

[8] *Id.*

This approach is also flawed because it adds to a growing list of disclosure about specific risks that may not be material to some companies and could make it seem like certain risks are more important than others. For example, requiring specific disclosures about cyber and climate risk management may signal to the investor that those are more important than other risks (e.g., competition risk). Also, if the SEC continues down this path of requiring disclosure of how specific risks are managed, it runs the risk of causing greater confusion—not greater clarity. As the Commission adds specific items to the list of required governance disclosures depending on the issue de jure, the disclosures will become less clear and easy to understand for investors. A better approach would be to expand the current corporate governance disclosure requirements to require a more detailed description of how boards are informed of risks generally instead of requiring disclosure of specific piecemeal topics.

III. CYBER INCIDENT REPORTING SHOULD BE STREAMLINED AT THE FEDERAL, STATE, AND INTERNATIONAL LEVELS

USTelecom urges the Commission to work with partners across the federal government, and also at the state level and with international partners, to avoid conflicting rules and ensure that regulations are minimally burdensome for reporting companies. We note that the recently enacted Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") calls for the formation of a Cyber Incident Reporting Council, led by the National Cybersecurity Director – and including among its participants the Office of Management and Budget ("OMB"), the Cybersecurity and Infrastructure Security Agency ("CISA"), and sector risk management agencies – to "coordinate, deconflict, and harmonize Federal incident reporting requirements".[9]

[9] CIRCIA § 2246.

In addition to being a full partner in U.S. driven incident reporting initiatives, the Commission should seek, at a minimum, to maintain awareness of international initiatives and incorporate them into its own strategic policymaking – avoiding disharmony to the largest extent possible. The Commission should also engage industry in these discussions. As noted above, not all industries are subject to the same requirements and there is potential for rules to be in direct conflict, even within the United States, which must be avoided at all costs.

Finally, we note that reporting information to government partners, while important, requires technical experts to focus on compliance with regulations during or in the immediate aftermath of a cyber incident. Any excess in interpretation or implementation of new rules risks diverting the limited and highly skilled cyber workforce away from operational cybersecurity efforts where they are needed. Again, engaging industry will be essential to ensure the rules are properly streamlined and effective, so as to maximize the resources devoted to mitigating and responding to cyber threats.

IV. A GENERAL REQUIREMENT TO DISCLOSE BOARD RISK MANAGEMENT BACKGROUNDS IS REASONABLE – FOCUSING EXCLUSIVELY ON CYBER EXPERTISE IS TOO NARROW

The Commission proposes to amend Item 407 of Regulation S-K, adding the new paragraph (j) requirement: "If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s) and provide such detail as necessary to fully describe the nature of the expertise."[10]

USTelecom would support general reporting about risk management backgrounds, but narrowing in on cybersecurity expertise does not take into account the diverse backgrounds and experiences that will contribute to a successful and diverse board.

[10] Proposed Rules at Part II (E) (1).

Companies are in the best positions to determine the makeup of the board, whereas the proposed rule incentivizes a cybersecurity check box over putting together the best board, including one that can adequately provide oversight of cyber risk management as well as other important initiatives for the company.

V. CONCLUSION

USTelecom appreciates this opportunity to comment on the Commission's proposed rules. We look forward to remaining engaged with the Commission on this matter of significance to our members, the broader cyber ecosystem, and the U.S. economy.

Respectfully submitted,

/s/ Paul Eisler

Paul Eisler
Senior Director, Cybersecurity

USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
[redacted]

May 9, 2022