TECHNET
THE VOICE OF THE INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

May 9, 2022

Ms. Vanessa Countryman
Secretary, Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

***Re: Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22)***

Dear Ms. Countryman:

TechNet appreciates the opportunity to submit written comments in response to the Securities and Exchange Commission's (SEC) notice requesting public feedback regarding the proposed rule on cybersecurity risk management, strategy, governance, and incident disclosure. TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over four million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

Securing intellectual property, safeguarding our economy and critical infrastructure, and protecting American consumers and businesses from cybersecurity risks has never been more important. World events, including Russia's unprovoked and heinous attacks on Ukraine, highlight the pressing need to defend against cyberattacks. In response, America's tech leaders are taking unprecedented steps to support Ukraine, isolate Russia, and ensure our national security, both overseas and here at home. With today's world growing more connected by the second, defending our critical infrastructure and protecting our data will require close collaboration between America's technology sector and the government.

Each cybersecurity intrusion puts the integrity of financial markets, national security, and utility services at risk, threatens businesses, especially small ones, and violates civil liberties through personal data theft and stolen identity. Per the Office of the Director of National Intelligence's 2021 Threat Assessment of the U.S. Intelligence Community, cybersecurity is among the top areas of concern for national security. TechNet realizes the urgency of improving our nation's cybersecurity resiliency and appreciates the seriousness of which the United States Government (USG) is approaching this matter.

Significant efforts have been taken by the USG to safeguard our critical infrastructure against cybersecurity threats. Currently, the White House Office of the National Cyber Director, National Security Council, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, the Department of Justice, Congress, and other federal agencies are doubling down on efforts to secure the nation's critical infrastructure. These efforts include implementing a statutory framework to report confirmed cyber intrusions, creating a unified and collaborative approach to encourage public/private information sharing, and making investments in the workforce to better equip Americans with the skills to fill the nearly 600,000 current open cyber positions.

The private sector, which owns or operates much of the country's critical infrastructure, remains critical to executing our country's overall cybersecurity strategy. The breadth of expertise and talent in the private sector can be used to help shape government processes and implement successful, cross-industry best practices. It is of the utmost importance for the USG to continue to recognize the numerous benefits that come from partnering with American businesses. As the SEC seeks to move beyond the 2018 Interpretative Release, TechNet appreciates the opportunity to provide constructive feedback and share our concerns with the proposed rule.

**Cyber Intrusion Prioritization**

Currently, a company's response to a cyber intrusion is to identify and remediate the invasion, collaborate with law enforcement and CISA, and determine the victims of the attack. The proposed rule implements a 4-day timeline to report intrusions to the SEC. This restrictive and arbitrary timeline forces the reallocation of valuable resources from mitigating the attack and protecting consumers' data to alerting investors. Relatedly, under the proposed rule, a public company would need to be able to assess whether a particular incident at a third-party service provider would have a material impact on the company and thereby trigger a Form 8-K filing. It is essential that companies have time to make this assessment as it takes a significant amount of time and effort to do this for acquisitions and other third-party services.

Providing accurate and holistic data to investors is important and should be done after a thorough investigation has been conducted to determine the attack is material, as prescribed in this proposed rule. The proposed rule, however, includes ambiguous examples of "material cybersecurity incidents" that seem to encompass many types of intrusions. Companies could be hurried in making the determination of a material intrusion based on incomplete information, therefore erring on the side of abundant caution and, as a result, deem more incidents as material than necessary. Premature disclosures of potential intrusions to the SEC could prove harmful to investors and the general public if the shared information is not fully

vetted and the incident is not remediated, potentially inviting additional cyberattacks.

**Burdensome Reporting Requirements**

Currently, every state has data breach notification laws that companies must follow. In addition, the USG is already implementing a reporting framework administered through CISA to aid and support companies within 72 hours of an intrusion. The additional reporting requirements proposed in this rule go far beyond the 2018 Interpretative Release and further complicate the compliance practices when a cyber intrusion occurs.

**New Item 106 of Regulation S-K and Amending Item 407 of Regulation S-K**

The proposed rule adds a new Item 106 of Regulation S-K that would oblige a registrant to disclose "the board's oversight of cybersecurity risk, management's role in assessing and managing such risk, management's cybersecurity expertise, and management's role in implementing the registrant's cybersecurity policies, procedures, and strategies." Furthermore, the rule proposes amending Item 407 of Regulation S-K "to require the disclosure of whether any member of the registrant's board has expertise in cybersecurity, and if so, the nature of such expertise."

The nature of these new requirements is ambiguous and the disclosure of board expertise in other areas is not required. While cybersecurity preparedness is important to investors, there are many other factors that impact stock prices, perhaps more drastically than a cyber intrusion. The benefits of this new reporting requirement appear unfounded and pose minimal benefit to investors while adding additional compliance burdens to companies.

**Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks**

The SEC's proposed rule includes "Item 106(b) of Regulation S-K to require registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy." The SEC further proposes "that disclosure of the relevant policies and procedures, to the extent a registrant has established any, would benefit investors by providing greater transparency as to the registrant's strategies and actions to manage cybersecurity risks." Further clarification on the use and application of this information would be critical to understanding the efficacy of this new requirement.

**Potential Disclosure of Proprietary Information**

Proposed Item 106(b) would "require registrants to disclose its policies and procedures, if it has any, to identify and manage cybersecurity risks and threats, including: Operational risk; intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk." Some of the information that falls under this

requirement could be privileged and confidential, and the benefit provided to investors by its public disclosure is unclear. At the same time, public disclosure of this sensitive information will provide malicious actors with details about companies' cyber risk management programs potentially increasing the risk of successful future cyber attacks.

TechNet appreciates this opportunity to submit comments to this proposed rule. Cybercrime cost the world economy nearly $1 trillion last year alone. As policies and regulations are created to meet the evolving technological landscape and the growing threat cyber attacks pose to our economy and infrastructure, it is important that new rules prioritize building a partnership with the private sector to strengthen the nation's cybersecurity resiliency.

**Response: If you have any questions regarding this comment letter, please contact Carl Holshouser, Senior Vice President, at [redacted].**