May 9, 2022

Submitted electronically via rule-comments@sec.gov

Ms. Vanessa A. Countryman
Secretary, Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: File Number S7-09-22: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Ms. Countryman:

Nareit[1] and The Real Estate Roundtable (The Roundtable)[2] appreciate the opportunity to submit these comments responding to the Securities and Exchange Commission's (SEC or Commission) March 9 proposal related to Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. (Proposal)[3]

Nareit, The Roundtable, and their members have long understood the critical importance of communicating accurate and material business and financial information, including material information about cybersecurity incidents and policies, to real estate investment trust (REIT) and other commercial real estate investors. We have also strongly supported efforts to promote understanding among commercial real estate participants of the nature of cybersecurity risks and policies to prevent and mitigate such risks.

Perspective on the Proposal

The Roundtable and Nareit have been strong supporters of policies that promote industry reporting to the federal government on significant cybersecurity incidents. The industry has also worked successfully since 2003 with federal law enforcement and intelligence agencies –

[1] Nareit serves as the worldwide representative voice for real estate investment trusts (REITs)[1] and publicly traded real estate companies with an interest in U.S. income-producing real estate. Nareit's members are REITs and other publicly traded real estate companies throughout the world that own, operate, and finance income-producing real estate, as well as those firms and individuals who advise, study, and service those businesses.
[2] The Real Estate Roundtable and its members lead an industry that generates more than 20% of America's gross national product, employs more than 9 million people, and produces nearly two-thirds of the taxes raised by local governments for essential public services. Our members are senior real estate industry executives from the U.S.'s leading income-producing real property owners, managers, and investors; the elected heads of America's leading real estate trade organizations; as well as the key executives of the major financial services companies involved in financing, securitizing, or investing in income-producing properties.
[3] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 87 FR 16590 (proposed March 9, 2022) at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

including the Cybersecurity and Infrastructure Security Agency (CISA) – to mitigate the risks associated with terrorism and criminal activity on a broad array of physical and cyber threats.

The real estate industry has also played an important role in fostering information-sharing practices between the U.S. government and the business community by creating the Real Estate Information Sharing and Analysis Center (RE-ISAC), a public-private information sharing partnership between the U.S. commercial facilities sector.[4] The RE-ISAC, has been designated by the Department of Homeland Security as the conduit for the commercial real estate industry for sharing information about potential physical and cyber security threats and vulnerabilities to help protect commercial facilities and the people who use them.

Nareit and The Roundtable are broadly supportive of the SEC's efforts to ensure that investors receive accurate and comparable material information regarding company cyber risk management and incidents. However, based on member feedback and analysis of the Proposal, we have a number of concerns arising from the detailed, granular reporting that would be required by the Proposal, and the rigid incident reporting deadlines, which members fear may unintentionally exacerbate cybersecurity risks for issuers and impose burdens unjustified by obvious benefits.

Executive Summary

- It is vital to harmonize SEC reporting requirements with other federal and state cyber incident reporting requirements.
- The Commission's proposed 72-hour reporting window should incorporate flexibility for a reporting delay to accommodate other law enforcement and other contingencies.
- Registrants should not be required to report detailed descriptions of their internal cybersecurity gameplans, which could compromise them in any number of ways.
- The prescriptive requirements for disclosing risk management, strategy, and governance regarding cybersecurity risk are burdensome and unjustified.

[4] The RE-ISAC, supported jointly by The Real Estate Roundtable and Nareit, has been designated by the Department of Homeland Security as the conduit for the commercial real estate industry for sharing information about potential physical and cyber security threats and vulnerabilities to help protect commercial facilities and the people who use them, as memorialized in a Cooperative Research and Development Agreement (CRADA) between the RE-ISAC and the Department of Homeland Security was executed on April 2, 2015.

Detailed Discussion

Harmonization with other Reporting Requirements.

Over the years, The Roundtable and Nareit have encouraged federal agency officials and lawmakers to work toward harmonizing duplicative and overly burdensome information security requirements that impact regulated businesses, including REITs and other commercial real estate firms. We believe that streamlining cybersecurity reporting requirements benefits real estate companies and their investors alike, by enabling firms to efficiently address cybersecurity matters and providing clarity to their investors, who are often confused by conflicting reporting to multiple governmental agencies.

For this reason, we respectfully suggest that as the SEC moves forward with its Cybersecurity Proposal, it work to ensure that its cybersecurity disclosure rules do not conflict with other state, federal, and (in several cases) international reporting requirements. Complying with duplicative and potentially conflicting cybersecurity reporting requirements is not only costly to companies, but may divert corporate resources needed to monitor on-going cyber risks and respond to a cyber-attack.

We believe that the recently enacted *Cyber Incident Reporting for Critical Infrastructure Act of 2022*[5], which will require critical infrastructure organizations to report cyber-attacks within 72 hours of reasonably believing that an incident has occurred, is particularly relevant to the SEC's Cybersecurity Proposal. The Act, which is intended to provide the federal government with a better understanding of the nation's cyber threats and facilitate a coordinated national response to ransomware attacks, will require CISA's Director to issue regulations covering, among other matters, the manner, timing and form of reports and the necessary steps to take for information preservation. We believe that it is important to ensure that the requirements of the SEC's Cybersecurity Proposal do not conflict with the requirements of this new law.

For these reasons, we urge the SEC to ensure that its cybersecurity disclosure framework is coordinated with other federal, state and local cybersecurity reporting requirements, policies and procedures. We also suggest that the SEC and other policymaking bodies engage in additional collaborative efforts with industry groups with the goal of streamlining corporate disclosure requirements arising from cyber incidents, to ensure that issuers are not distracted by unnecessary requirements and that investors are not confused by duplicative and confusing reporting.

[5] On March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the "Act"), creating new requirements for organizations operating in critical infrastructure sectors to report to the federal government certain cyber incidents and related ransom payments. The Act is part of the Consolidated Appropriations Act, 2022 (H.R. 2471). This Act reflects a renewed regulatory focus on cybersecurity risks as cyber threats intensify.

Nareit and The Roundtable look forward to working constructively with the SEC and other federal and state agencies to find a balanced approach to providing investors with meaningful, material cybersecurity risk disclosure and protecting American businesses from cyber-attacks while not imposing burdensome regulations on the industry.

Reporting Window Should Accommodate Law Enforcement and other Contingencies.

The Roundtable and Nareit support reasonably timed and flexible cyber incident reporting to the relevant federal, state and local governmental entities. However, based on discussions with our members, we believe that the Proposal's rigidly conceived four-business-day window to disclose material cybersecurity incidents raises several concerns for REITs and other issuers. Of greatest concern, the Proposal would not provide any flexibility to delay incident reporting because of an ongoing internal or external investigation, including one directed by federal or state law enforcement officials, related to the cybersecurity incident.

As an initial matter, upon discovering a cyber incident, many companies may not immediately have comprehensive awareness of the facts and implications of the breach, particularly in the common circumstance of a rapidly evolving cyber incident taking place over several days. Companies may also not be in a position to assess the materiality of the breach within 72 hours, because it may need additional time to determine the nature and magnitude of the attack and the implications for the company's operations. Requiring premature disclosure in such circumstances would effectively force many companies to file a series of sequentially updated reports to the SEC, many of limited utility to investors, or worse, confusing to them. Moreover, diverting critical resources to continuously update disclosure may diminish the effectiveness of the actual response and mitigation efforts.

Further, our members also point out that requiring a company undergoing a ransomware attack to report the incident prematurely could exacerbate injury to the company, especially if the disclosure occurs when an intruder is still present in the company's network. We are also concerned that requiring issuers to make a rapid-fire, though incomplete or inconclusive, cyber disclosure based on fragmentary information may also expose issuers to additional liability and reputational and litigation risk.

Many REITs and other landlords lease space to federal and state government agencies, including some with national security missions. These leasing arrangements are often subject to cybersecurity monitoring and incident reporting regimes that are specific to the nature of the facility, the government tenant, or to the location. Because the Proposal's rigid reporting requirements are not coordinated with other governmental reporting regimes, these REITs and other landlords are likely to be confronted with reporting requirements that are, at best duplicative and burdensome, and at worst, conflicting and irreconcilable.

We also have concerns that the requirement that issuers make a disclosure to the SEC when "… a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate" is vague and unworkable. The process of assessing materiality of a series of prior (and perhaps current) incidents in the aggregate would pose significant burdens, forcing companies to expend considerable resources to continuously reevaluate prior events. Moreover, some have raised concerns that reclassification of a prior incident as material in hindsight could give rise to the perception that the issuer failed to properly assess materiality upon prior discovery.

In light of these concerns, we urge the SEC to incorporate flexibility in the 72-hour reporting window set forth in the Proposal. At minimum, the SEC's proposed cybersecurity rule should include a workable procedure for providing an issuer with a reporting delay upon request, when accompanied by a request from a law enforcement or national security agency.[6] Moreover, the reporting window should also include procedures to accommodate circumstances when disclosure within 72 hours would exacerbate injury to the company and/or its shareholders. We also urge the SEC to reconsider the requirements related to reporting prior immaterial cyber incidents, which we believe impose burdens and potential liabilities, without benefit.

Registrants should not be required to report detailed descriptions of their internal cybersecurity gameplans, which could compromise them in any number of ways.

Both of our organizations support disclosure of relevant and material information about issuer cybersecurity risk management policies and procedures. However, we have significant concerns with the provisions of the Proposal that would require issuers to make detailed disclosure of their policies, procedures, and methods for identifying and managing cybersecurity risks, because such disclosures may lead to a degradation of their cybersecurity programs and expose their companies to a range of risks posed by a range of bad actors.

In particular, we believe that issuers should not be required to disclose sensitive details about their cybersecurity monitoring and response programs in SEC filings. Such disclosures may heighten exposure to cyber-attack, or otherwise compromise enterprise response.

We also note that many issuers rely on third-party cybersecurity experts and vendors to assist in the development and maintenance of their cybersecurity policies and procedures. Requiring detailed disclosure of these proprietary systems and programs may be contrary to contractual obligations to protect the intellectual property, or other rights of these third parties.

[6] We note that the Exchange Act currently recognizes circumstances when national security concerns temporarily exempt issuers from certain reporting requirements. 15 U.S.C. 78m (b)(3)(A). Because issuers typically experience cyber incidents in pressured time frames, we recommend that the SEC develop a practical procedure that incorporates this principle as it moves forward with its Cybersecurity rulemaking.

***Proposal's Required Disclosure of Cyber Risk Management, Strategy & Governance is Burdensome and unjustified*.**

Nareit and The Roundtable agree with the SEC that REITs and commercial real estate issuers, together with all issuers, must have robust processes and internal controls in place to manage and report on cybersecurity risk and incidents, together with board competence to oversee these processes. But we are concerned about the highly prescriptive nature of the requirements set forth in the Proposal and the "one size fits all" presumption that the prescriptive requirements will be appropriate for all industry sectors.

As an initial matter, we are concerned that the Proposal's requirements that issuers disclose policies, procedures, and granular information about management roles and responsibilities creates significant pressure to conform internal processes and controls in a manner that may be inappropriate for an any given issuer and of no material benefit to the issuer's investors. We believe that disclosing this level of detail does not benefit investors and is likely to be misleading to investors. We are similarly concerned that the requirements that issuers disclose how—and when—the board considers cybersecurity risks in detail is not beneficial to investors and may, again, provide useful information to cyber-criminals.

We have similar concerns about the Proposal's requirement that issuers disclose the cybersecurity expertise of directors and management. We fear that this will pressure companies to hire "cyber experts" of unproven value to the company, simply to "check the box." We note that the Proposal suggests that companies should consider whether directors, or relevant managers, have obtained a certification or degree in cybersecurity, which raises additional concerns. Because there is no commonly accepted credentialling, or credentialling body, for a "cyber expert," the presence or absence of such a designated expert may mislead investors. Further, as many others point out, there is a limited supply of cybersecurity experts of whatever credentials, suggesting that this requirement inevitably sets many companies up for immediate failure.

Conclusion

Nareit and The Roundtable appreciate the opportunity to submit these comments on this important topic and stand ready to work directly with the Commission as it moves forward to develop a clear, transparent and secure set of cybersecurity disclosure rules.

We trust that the Commission will find our comments helpful. Should you have questions or require additional information, please contact Victoria Rostow at Nareit by telephone at [redacted] or by email at [redacted]; or Clifton E. Rodgers, Jr. at The Real Estate Roundtable by telephone at [redacted] or by email at [redacted].

Nareit
Real estate working for you.

The Real Estate Roundtable

Thank you for the opportunity to comment on this important issue.

Respectfully submitted,

Steven A. Wechsler
President & CEO
Nareit

Jeffrey D. DeBoer
President & CEO
The Real Estate Roundtable