May 9, 2022

Submitted electronically via SEC.gov

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

Dear Ms. Countryman:

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

NMHC and NAA appreciate the opportunity to submit these comments responding to the Securities and Exchange Commission's (SEC or Commission) March 9 Proposed Rule related to Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.[1] We endorse a single, flexible regulatory scheme concerning data security and incident notification. We also support a balanced approach to providing investors with meaningful insight into a business's operations, including material cybersecurity risks and incidents, while not imposing overly burdensome regulations on the apartment industry or unintentionally exposing our members to substantially greater cybersecurity risks.

For more than 25 years, the National Multifamily Housing Council[2] (NMHC) and the National Apartment Association[3] (NAA) have partnered to provide a single voice for America's apartment industry. Our combined memberships are engaged in all aspects of the apartment industry, including ownership, development, management and finance. NMHC represents the principal officers of over 1,500 firms that own, develop, manage and finance apartments. As a federation of more than 145 state and local affiliates, NAA encompasses over 73,000 members representing nearly 9 million apartment homes globally. The apartment industry today plays a critical role in housing this nation's households by providing apartment homes to 40.1 million residents, contributing $3.4 trillion annually to the economy while supporting 17.5 million jobs. In addition to public companies, our members also include investment advisors and investment funds.

Perspective on the Proposal

NMHC and NAA and their collective members understand the critical importance of maintaining the integrity of the highly sensitive data collected, used, and maintained to support applicants, residents, and employees in the apartment industry. In the course of doing business, rental housing owners and operators, and their third-party service providers, collect, use, and maintain a significant amount of highly sensitive personal data about applicants, residents, and employees.

[1] 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.
[2] The National Multifamily Housing Council is a non-profit trade and advocacy group for the apartment industry, available at https://www.nmhc.org/.
[3] The National Apartment Association is a non-profit trade association of apartment communities, owners and vendors, available at https://www.naahq.org/.

This information is used in a wide variety of essential business operations but also makes apartment firms a target of malicious actors.

Given the ever-expanding cyber-threat landscape, the apartment industry has made defense against these vulnerabilities a top priority. We have undertaken efforts within the apartment industry to mitigate cybersecurity risks, to implement policies to prevent and mitigate such risks, and to encourage investments in bolstering cyber defenses to protect data. To those ends, we have commissioned white papers on the threat landscape and provide resources and best practices for the apartment industry.

NMHC and NAA are broadly supportive of the SEC's efforts to American businesses to bolster cybersecurity and to ensure that investors receive comparable material information regarding companies' cyber risk management and incidents. However, our comments provided herein concern specific elements of the Proposed Rule that are overly burdensome given the complexity of cybersecurity incidents and that may result in increased cyber risks and liability for public companies.

Executive Summary

The Proposed Rule imposes overly burdensome requirements and requires companies to assume unnecessary, but significant, legal and cybersecurity risks. The following details our concerns, which are addressed in more depth in the "Detailed Discussion" section below:

1. **The Proposed Rule's detailed reporting requirement concerning a company's cybersecurity risk management policies and procedures unnecessarily exacerbates cybersecurity risks.**

2. **The broad scope of the Proposed Rule's reporting requirements at the time of an incident and in subsequent quarterly and annual reports are overly burdensome.**

3. **The disclosure of a "material cybersecurity incident" before the threat actor has been fully neutralized can create additional vulnerabilities and legal risks for a company.**

4. **The Proposed Rule fails to provide clear direction regarding how a company should evaluate the cybersecurity practices of third-party service providers.**

5. **The Proposed Rule does not include a comprehensive safe harbor provision, which is necessary to encourage disclosure and best efforts to meet compliance standards.**

Detailed Discussion

1. **Detailed Disclosure of Cybersecurity Risk Management Policies and Procedures Enhances Cybersecurity Risks.** The Proposed Rule amends several of the Commission's quarterly and annual reporting forms and rules (Forms 10-K, 10-Q, 20-F, 8-K, or 6-K and

Regulation S-K) for public companies to require additional cybersecurity-related information to be disclosed publicly to potential investors.[4] The Proposed Rule would add disclosure requirements regarding cybersecurity incidents, cybersecurity risk management policies and procedures, and cybersecurity governance, including oversight and cyber expertise of the Board of Directors.[5]

In an effort to achieve "greater transparency," the Proposed Rule seeks to require registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy.[6] The Proposed Rule, thus, requires a description of a registrant's cyber risk assessment program and activities undertaken to prevent, detect, and minimize cybersecurity incidents, as well as how cybersecurity incidents have or are likely to affect the registrant's strategy, business model, results of operations, or financial condition and how cybersecurity risks are part of the business strategy, financial planning, and capital allocation.[7] Such specific and detailed public disclosures unintentionally and unnecessarily identify a company's cybersecurity vulnerabilities and enhance a company's cybersecurity risks. It would be naïve of us to dismiss such disclosures are more valuable to investors than cybercriminals, who will likely use this publicly available information in designing targeted attacks. Indeed, what is transparent to an investor will be transparent to sophisticated cybercriminals and nation-state actors.

NMHC and NAA support the disclosure of relevant, high-level information about an issuer's cyber risk management policies and procedures; however, registrants should not be required to report detailed descriptions of their internal cybersecurity plans, which could compromise their defenses. A company's cyber risk management and strategy can be summarized at a high-level without disclosing the level of detail sought by the Proposed Rule. Therefore, we urge the SEC to revise the required disclosures in proposed Item 106(b) of Regulation S-K to provide a general, high-level understanding of the attention and resources dedicated to cybersecurity without the details of the cybersecurity program and its strategies, activities, and defenses

2. **The Incident Reporting Requirements Are Overly Burdensome and Require Greater Flexibility.** The Proposed Rule requires public disclosures of material cybersecurity incidents within four business days after a registrant determines that it experienced such an incident. In addition, registrants are required to provide periodic updates concerning the material cybersecurity incident. These disclosures require detailed information about the cybersecurity incident, including whether data was stolen, altered, accessed, or used for any other unauthorized purposes.

[4] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 87 FR 16590 (proposed March 9, 2022) at 18-20, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[5] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 87 FR 16590 (proposed March 9, 2022) at 55, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[6] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 87 FR 16590 (proposed March 9, 2022) at 35, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[7] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 87 FR 16590 (proposed March 9, 2022) at 107, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

The scope and timing of this incident reporting requirement are overly burdensome and unnecessarily prescriptive. Upon discovering a cybersecurity incident, companies immediately dedicate resources to contain, investigate, and eradicate the threat. Forensics investigations of a cybersecurity incident are often conducted in anticipation of litigation and under attorney-client and work product privilege. While these efforts are underway, most companies do not have a comprehensive awareness of the facts or the implications of the breach. Requiring detailed cybersecurity incident disclosures, especially within a short window, pulls resources away from these efforts and could result in an unintentional waiver of privilege. As the investigation continues to discover new information, this could result in a cascade of additional reporting obligations. Moreover, prior disclosures may no longer be accurate, which could require constant corrections and could result in potential liability if deemed misleading.

The Proposed Rule also applies to an incident involving "information resources owned or used by the registrant." Thus, registrants are also responsible for making a materiality decision for incidents involving third-party systems.[8] This requirement is overly broad and burdensome to registrants who do not control or have access to these information systems.

Additionally, the lack of harmonization amongst the various incident reporting obligations is burdensome, especially for smaller businesses. Apartment firms increasingly operate across multiple states and must comply with a patchwork of 50 different state laws governing data security and breach notifications, various federal cybersecurity incident reporting requirements, and potentially foreign laws. The lack of harmonization amongst these governmental entities increases costs and causes confusion as agencies and consumers receive notifications at different times concerning the same cybersecurity incident.

NMHC and NAA urge the SEC to consider greater flexibility with reporting cybersecurity incidents to reduce burdens on companies, especially concerning the details sought and the constant periodic reporting obligation. Moreover, NMHC and NAA encourage the SEC to harmonize its cybersecurity incident disclosure obligations to be consistent with other federal agencies and state laws.

3. **Registrants should not be required to report a "material cybersecurity incident" publicly until the threat actor has been neutralized.** Under the Proposed Rule, public disclosure of an incident will be required in many circumstances before the threat is contained or eradicated, which can complicate a company's response to the cybersecurity incident as well as expose it to additional cybersecurity and legal risks. For instance, a company subject to a ransomware attack may be obligated to publicly disclose the "material cybersecurity incident" while negotiating with the cybercriminals, which could significantly undermine its negotiation position and enhance the cybercriminals bargaining power. Alternatively, a company whose backups are not fully operational within this 4-day window may feel compelled to pay a ransom demand before public disclosure of the "material cybersecurity incident," which would result in unnecessary and costly payments.

[8] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 87 FR 16590 (proposed March 9, 2022) at 31, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

During the initial stages of a cyberattack, a company will aim to ensure that the threat has been contained and eradicated before safely rebuilding its systems and restoring operations. Public disclosure of a cybersecurity incident before eradication and remediation could create opportunities for cybercriminals to further target the victim company. Moreover, such public disclosures, without specifics that the threat has been eradicated and systems remediated, may result in speculative trading. The "one size fits all" reporting period, thus, may create unintentional and negative consequences. We urge the SEC to allow companies an appropriate opportunity to contain and eradicate cyber threats before requiring public disclosures of material cybersecurity incidents.

4. **Provide clear guidance concerning oversight of the cybersecurity practices of third parties.** The apartment industry relies heavily on third parties not just for IT but also for numerous services (e.g., physical security systems, rental payment systems, employee payroll, embedded smart technologies, etc.). These third-party vendors and service providers often collect, use, and maintain vast amounts of sensitive data about residents, prospective residents, and employees. As the apartment industry does not own or have access to the IT systems employed by these vendors and service providers, monitoring and evaluating third parties' cyber hygiene continues to be a significant challenge.

   Although the Proposed Rule would require disclosure of a registrant's policies and procedures to oversee and identify cybersecurity risks associated with third-party service providers,[9] it does not provide any parameters or guidance on how companies should conduct such activities. This third-party disclosure requirement imposes a significant legal risk to a registrant as statements concerning its practices could become a potential basis for litigation and/or enforcement action if a third-party service provider experience a material cybersecurity incident. The lack of clear SEC guidance on adequate oversight only enhances the challenges that companies face with monitoring and evaluating third parties' cyber hygiene. Therefore, if the SEC requires companies to disclose its policies and procedures to oversee and identify cybersecurity risks associated with third-party service providers, it should provide clear guidance for evaluating a third party's cybersecurity practices. Moreover, if a company had conducted an adequate evaluation process of the third-party service provider, incident reporting requirements concerning third-party information systems should carry a safe harbor for registrants with respect to SEC enforcement actions and securities litigations.

5. **Provide more extensive liability protections and safe harbor provisions.** The Proposed Rule requires registrants to publicly report material cybersecurity incidents within four business days after determining that a material cybersecurity incident has occurred. Because management must make a rapid materiality determination to meet this requirement, the Proposed Rule extends a limited safe harbor rule for the failure to timely report a material cybersecurity incident.[10]

   However, this safe harbor is significantly limited. Although cybersecurity incidents are complex and constantly evolving, the Proposed Rule provides no litigation protection against

[9] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 87 FR 16590 (proposed March 9, 2022) at 36, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[10] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 87 FR 16590 (proposed March 9, 2022) at 27-28, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

inaccurate statements caused by rapidly reporting material cybersecurity incidents within the four-day window and often before an investigation is completed. It also provides no protections related to the other disclosure requirements, such as information regarding a company's cybersecurity risk management policies and procedures. As noted earlier, the Proposed Rule offers no liability protection to registrants when third-party service providers experience a material cybersecurity incident.

In addition, most state data breach laws provide a safe harbor provision to permit delayed notifications when law enforcement determines that such notices will impede an investigation. However, the Proposed Rule does not adopt a similar approach even though publicly reporting a cybersecurity incident could undermine these states' safe harbor provisions and potential law enforcement investigations.

We strongly recommend the SEC consider expanding protections and safe harbors to companies reporting cybersecurity incidents and their cybersecurity risk management policies and procedures, especially related to third-party information systems. Without such protections, the Proposed Rule may result in increased costs borne upon the apartment industry, which would affect housing affordability.

Conclusion

NHMC and NAA 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 Cindy Chetti, NMHC Senior Vice President, Government Affair via email at cchetti@nmhc.org or cell phone at 703-395-0469.

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

Respectfully,

Cindy V. Chetti
Senior Vice President, Government Affairs
National Multifamily Housing Council

Gregory S. Brown
Senior Vice President, Government Affairs
National Apartment Association