May 5, 2022

Via E-mail to rule-comments@sec.gov

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

Re: Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File No. S7-09-22)

Dear Ms. Countryman:

We appreciate the opportunity to respond to the U.S. Securities and Exchange Commission’s (the “Commission” or “SEC”) request for comments on the proposed rule on Cybersecurity Management, Strategy, Governance, and Incident Disclosure (the “Proposed Rule”). This comment focuses on the potential adverse consequences of requiring disclosure of cybersecurity incidents that are not publicly known and not remediated.

Empire State Realty Trust, Inc. (“ESRT” or “we”) is a self-managed REIT that operates a portfolio of office, retail, and multifamily properties, including the world-famous Empire State Building office and observation deck, in Manhattan and the greater New York metropolitan area. ESRT has been registered with the SEC as a publicly-traded company since 2013 and its shares are listed on the New York Stock Exchange. Like other companies in our business lines, we rely extensively on technology, both internal and outsourced, to process transactions and manage our business, so our business is increasingly at risk from cyberattacks that continue to increase in number, intensity and sophistication. A cyberattack can compromise the confidential information of employees, tenants, customers and vendors, and disrupt business operations and relationships. Any compromise of security can also result in a violation of applicable privacy and other laws, with damage to legal and financial condition, reputation and records. Further, information systems may be considered to be susceptible to a future terrorist attack.

On March 9, 2022, the Commission issued the Proposed Rule to “enhance and standardize disclosures” regarding, inter alia, cybersecurity incident reporting by public companies, including by requiring current reporting on cybersecurity incidents within four business days of a registrant determining that the incident was “material.” Critically, there is no carveout or flexibility for reporting non-public incidents that have not been remediated or that involve law enforcement. We appreciate the Commission’s desire to address the “concern that material cybersecurity incidents are underreported and that existing reporting may not be sufficiently timely.” However, by requiring disclosure of non-public cybersecurity incidents with active, unremediated vulnerabilities, the Proposed Rule carries a risk of unintended, adverse consequences for the investing public. As explained further below, disclosing unremediated vulnerabilities can result in cyberattacks within hours of disclosure, which in turn can cause significant financial damage to a
company and its shareholders. ESRT therefore requests that the Commission consider and address the issues discussed below in order to mitigate this risk.

**Reporting of Cybersecurity Incidents On Form 8-K**

The proposed timing for reporting material cybersecurity incidents does not distinguish between active versus remediated incidents, or between non-public and publicly-known incidents, and would therefore require public disclosure of non-public and unremediated vulnerabilities. Although we acknowledge the importance of promptly disclosing cybersecurity incidents, there are certain scenarios—such as when an incident is not publicly known and has not been remediated—where public disclosure may risk exposing registrants to additional cyberattacks or thwart law enforcement. And, depending on the nature of the incident and the affected registrant, this risk may trickle down or up to other registrants and companies, including vendors such as cloud service providers, and even the federal government. Avoiding forced pre-mature disclosure under such circumstances allows a company to provide more accurate and complete information to investors, and thus aids, rather than undermines, the SEC’s goal of protecting investors by providing information that is material to their investing decisions.

**Current Reporting Timeline**

The Proposed Rule would require a registrant to report a cybersecurity incident within four business days of determining that it is “material.” The definition and examples of what would constitute a material incident appear to sweep in virtually all cybersecurity incidents, including, *inter alia*, data/system/network breaches and/or vulnerabilities, ransomware attacks, and even threats or offers to publicly disclose sensitive company data.1 As such, it appears that the SEC expects that a materiality determination will be made on or near the date of discovery—e.g., when one of the enumerated examples of material incidents occurs. The proposal previews this by explicitly stating that “[i]n some cases, the date of the registrant’s materiality determination may coincide with the date of discovery of an incident.”2 As a practical matter, the Proposed Rule would thus frequently require disclosure of material incidents within four business days of the date of discovery. This timeline is too short. In many situations, four days may not be sufficient to fully understand the extent of the incident to determine materiality, much less enough time to contain or remediate the underlying vulnerability. Indeed, the four-day disclosure timeline would require that registrants disclose incidents approximately three months earlier than the average time recent studies have shown it takes companies to contain cyber incidents and more than 6 months before they typically can remediate vulnerabilities.3

---


2 Proposed Rule, p. 22.

3 A study sponsored and published by IBM Security found that the average time to contain a data breach in 2020 was 73 days, but was high as 93 days for the public sector and healthcare industries. See IBM Security, *Cost of a Data Breach Report (2020)*, pp. 52, 54 available for download at https://www.ibm.com/downloads/cas/RZAX14GX. Another study found that an average time of 202 days was needed to fix cybersecurity vulnerabilities as of the first half of 2021. See David Bisson, *High-Severity Vulnerabilities Now Take Nearly 250 Days to Remediate, Survey Finds*, SECURITY INTELLIGENCE, September 29, 2021, https://securityintelligence.com/news/news-vulnerabilities-25-days-remediate/
Potential Harms to Investors

In addition to requiring public disclosure of non-public unremediated cybersecurity incidents or vulnerabilities, the Proposed Rule would also require a registrant to disclose whether it “has remediated or is currently remediating the incident.” There are at least two risks associated with this requirement.

First, it potentially exposes the reporting registrant to additional cyberattacks by informing threat actors that the company’s information system is vulnerable. Studies have shown that threat actors are actively and continuously scanning for vulnerable systems. As one security researcher put it, “adversaries are opportunistic predators, constantly searching for vulnerable targets to attack.”

Furthermore, industry experts have warned that even generic disclosures, without technical details about the underlying vulnerability, can expose a company to cyberattacks. In fact, “the mere knowledge of a vulnerability’s existence in a feature of some product is sufficient for a skillful person to discover it for themselves. Rumor of a vulnerability draws attention from knowledgeable people with vulnerability finding skills—and there is no guarantee that all those people will have users’ best interest in mind.”

Second, premature disclosure may interfere with active investigations by law enforcement, and the Proposed Rule does not contain any mechanism to delay reporting incidents in such circumstances. This issue is particularly salient for companies that operate critical infrastructure and/or in the national security arena.

Responsible Disclosure

The Proposed Rule would require a registrant to disclose material cybersecurity incidents on information systems “owned or used by the registrant.” Past examples have shown that public disclosure of unremediated vulnerabilities can result in cyberattacks within hours of disclosure against an unlimited range of targets. Hence, requiring a registrant to disclose in a matter of days an incident on a third-party service provider’s system could potentially result in attacks against the vendor and their enterprise customers (many of whom may themselves be registrants) well before they are able to implement mitigation. Additionally, disclosing a vulnerability in one vendor’s system can expose vulnerabilities in the same components used by other vendors. This risk is particularly relevant where the vulnerable component is widely used. For example, a vulnerability known as “Meltdown,” which was discovered in 2018, reportedly “affect[ed] almost all computers,

---


6 Id.

7 For example, a vulnerability known as “Shellshock,” or “Bashdoor” which affected Linux-based products, was discovered and disclosed in September 2014; and “within hours of the release of this bug to the general public, attackers reportedly exploited this vulnerability to create botnets on compromised computers to perform DDoS (distributed denial-of-service) [attacks] and vulnerability scanning.” European Union Agency for Cybersecurity (ENISA) Good Practice Guide on Vulnerability Disclosure, p. 11, n.2, November 2015, https://www.enisa.europa.eu/publications/vulnerability-disclosure.
servers, cloud operating systems and cell phones made in the past two decades.” The recent critical vulnerability known as “Log4J” was similarly far-reaching, impacting “tens of thousands of software packages … and projects across the software industry.” Log4J was disclosed to the public in December 2021 and has since been “highly exploited in the wild,” reportedly used by state-sponsored hackers from China, Turkey, Iran and Turkey, and deployed to launch cyber-attacks against high profile targets including Belgium Ministry of Defense and Onus, one of Vietnam’s largest cryptocurrency trading platforms.10

By requiring a registrant to unilaterally disclose an unremediated vulnerability on a third-party system, the Proposed Rule may upend the establish practice of responsible disclosure of vulnerabilities—also known as Coordinated Vulnerability Disclosure (“CVD”)—which is considered industry best practice, and is endorsed by the federal government11 and international security organizations.12 The hallmark principle of the CVD process is that vulnerabilities should not be publicly disclosed until a fix is available. Therefore, when a researcher discovers a vulnerability, she or he confidentially reports it to the vendor who is responsible for developing a fix and they agree to an “embargo period”—during which time the vulnerability is kept a secret to allow vendors to release security updates or mitigations and workarounds to protect customers. Importantly, the European Union Agency for Cybersecurity has provided guidance making clear that “[t]here is no single universally appropriate timeframe for investigating andremedying security vulnerabilities.”13 And, as Richard Prethia, director of SEI/CMU, CERT Division, explained in his testimony before the US Senate, “the best way to . . . improve the security of [] systems is to work with . . . technology producers and vendors to develop workarounds and repairs for security vulnerabilities disclosed to the CERT/CC. To this end, in the absence of a major threat, we do not publicly disclose vulnerabilities until a repair or workaround has been developed, along

---

13 ENISA Good Practice Guide on Vulnerability Disclosure, supra, p. 60.
14 CERT refers to the Computer Emergency Response Team Coordination Center for the Carnegie Mellon University Software Engineering Institute (CMU/SEI), which is a non-profit research and development center that is funded by the US federal government. https://www.sei.cmu.edu/about/index.cfm. CERT is a leading authority in cybersecurity, partnering with the US government, industry, law enforcement and academic institutions in order to counter large-scale, sophisticated cyber threats. CERT/CC is one of a handful of national coordinators and prioritizes coordinating efforts around vulnerabilities that affect multiple vendors or that impact safety, critical or internet infrastructure, or national security. See https://www.kb.cert.org/vuls/; see also https://irp.fas.org/congress/1996_hri/s960605m.htm.
with directions on how to install it. ”15 In short, the Proposed Rule would conflict with responsible disclosure of vulnerabilities, which would ultimately harm the investing public by increasing the cybersecurity risks for the reporting registrants, other public companies, and their service providers.

**Recommendations**

In order to address and mitigate the above concerns, the SEC should consider revising the Proposed Rule to permit flexibility in the reporting timeline where a reportable incident (i) is not publicly known; and (ii) is not contained, has unremediated vulnerabilities, is subject to a pending law enforcement investigation and/or pursuit of the threat actor(s), or occurs on an information system used (but not owned) by the registrant.

***

We appreciate this opportunity to provide comments on the Proposed Rule for the Commission’s consideration, and welcome further discussion if helpful.

Sincerely,

________________

Thomas N. Keltner
Executive Vice President and General Counsel
Empire State Realty Estate Trust, Inc.

---

15 Carnegie Mellon University Software Engineering Institute Testimony of Richard Pethia Manager, Trustworthy Systems Program and CERT Coordination Center Software Engineering Institute Carnegie Mellon University Before the Permanent Subcommittee on Investigations U.S. Senate Committee on Governmental Affairs, June 5, 1996, [https://irp.fas.org/congress/1996_hr/s960605m.html](https://irp.fas.org/congress/1996_hr/s960605m.html). The US Cybersecurity and Infrastructure Security Agency (“CISA”) echoes this principle, noting that the timeframes for disclosing vulnerabilities is dependent on a number of factors, including, among other things, the “availability of effective mitigations” and “vendor estimate of time required for customers to obtain, test and apply the patch.” CISA also explains that CISA “may work with vendor(s) to facilitate time for affected end users to obtain, test, and apply mitigation strategies prior to public disclosure.” [https://www.cisa.gov/coordinated-vulnerability-disclosure-process](https://www.cisa.gov/coordinated-vulnerability-disclosure-process).