May 9, 2022
Via https://www.sec.gov/rules/submitcomments.htm

Vanessa A. Countryman, Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-0609

Security and Exchange Commission proposed rule regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, File S7-09-22

Dear Secretary Countryman:

Tenable Holdings, Inc. submits these comments in response to the Securities and Exchange Commission’s (“SEC”) proposed rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.¹ (the “proposed rule”). Tenable appreciates the opportunity to submit comments and believes that the commentary offered will be helpful to the SEC in providing additional information from the cybersecurity industry’s perspective on several key elements of the proposed rule. We write in overall support of the proposed rule, with more detailed comments to ensure the final rule meets the SEC’s stated goals.

Tenable is headquartered in Columbia, Maryland. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world’s first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and standards throughout the global community.

Tenable commends the SEC for its initiative and ongoing efforts to enhance and standardize disclosures regarding cybersecurity, and strongly supports the SEC’s proposed rule that will require public companies to disclose their policies and procedures for

¹ https://www.sec.gov/rules/proposed/2022/33-11038.pdf
identifying and managing cybersecurity risks, management’s role in implementing cybersecurity policies and procedures, and the board of directors’ cybersecurity expertise.\textsuperscript{2} We believe it is important that investors know whether a registrant’s board of directors has an oversight role regarding cybersecurity governance, including its oversight role regarding cybersecurity risks. Tenable also supports the SEC’s proposal to require disclosures of cyber incidents with the specific feedback and input included in comments submitted by the Cybersecurity Coalition (attached to this submission).

We recognize the importance of providing decision-useful and relevant information to investors to facilitate informed investment decisions. Requiring increased transparency around cybersecurity risk management practices is critically important for shareholders to make informed decisions about their investments. Shareholders should have access to information about whether public companies are taking action to address cybersecurity risks and the negative impacts of cybersecurity breaches.

Cybersecurity breaches can damage a company’s financial condition. In addition to the costs of remediation from a cyberattack and loss of customers, revenue and reputation, there are risks of shareholder lawsuits, customer lawsuits, increases in insurance premiums and increased scrutiny from external auditors and regulators. Additional consequences of cyber failures include distraction of management, which can result in new problems unrelated to the breach; the trigger of customer audits of a company’s cybersecurity defenses, which can lead to the involvement of outside counsel and other third parties; and significant expenses, among others.\textsuperscript{3}

In addition, the proposed disclosure requirements would dramatically improve our cybersecurity preparedness as a nation. We believe that requiring greater transparency of cyber risk practices and oversight forces companies to treat cybersecurity risk as business risk, leading to stronger cybersecurity governance and accountability among corporate leaders and boards and, ultimately, more effective cybersecurity. We strongly believe that this proposal serves as the most significant driver

\textsuperscript{2} This was a key recommendation of the Cyberspace Solarium Commission to strengthen the broader cyber ecosystem, https://www.solarium.gov/report.

\textsuperscript{3} Tenable General Counsel Steve Riddick, Harvard Business Review Article, https://hbr.org/2021/09/the-sec-is-serious-about-cybersecurity-is-your-company
for inciting corporate leadership to pay attention and establish baseline cybersecurity practices and processes.

Detailed below are Tenable’s responses to specific questions as numbered within the proposed rule.

**Question 17.** Should we adopt Item 106(b) and (c) as proposed? Are there other aspects of a registrant’s cybersecurity policies and procedures or governance that should be required to be disclosed under Item 106, to the extent that a registrant has any policies and procedures or governance? Conversely, should we exclude any of the proposed Item 106 disclosure requirements?

We recommend the adoption of Item 106(b) and (c) with the following changes bolded and in brackets:

1) **item 106(b)(i):** The registrant has a cybersecurity risk assessment program [that continuously assesses cybersecurity risks and implements safeguards designed to control those risks] and if so, provide a description of such program.

Tenable believes it would be useful for investors to know if a registrant’s cybersecurity risk assessment program includes continuous assessments of cybersecurity risks vs. periodic assessments of cybersecurity risks. If a registrant only assesses cybersecurity risks on a periodic basis, such as once per month or once per quarter, the organization is at greater risk of an exploitation than if a registrant continuously assesses cybersecurity risks. Today’s threat landscape is highly dynamic and requires organizations to continuously assess and defend against new tactics, techniques and procedures (TTPs) used by threat actors and cyber criminals. We have also observed dramatic decreases between when a new vulnerability is discovered and when it is leveraged in widespread attacks. Periodic assessments of cybersecurity risks would significantly inhibit an organization’s ability to respond quickly and effectively to remediate or mitigate these threats.

In addition, it would be useful for investors to know whether the registrant’s risk assessment program includes actions to control or mitigate those risks. As stated above, there are significant costs associated with the remediation from a cyberattack and
cybersecurity breaches can damage a company’s financial condition. Knowing whether a registrant has plans to control or mitigate cybersecurity risks is necessary for investors to make an informed decision about their investment. It would also be useful for organizations to communicate and track their cybersecurity risk profile using specific key performance indicators (KPIs) to provide additional transparency to investors. Cybersecurity risk should be another metric used by the financial services community to manage risk and incorporate into strategic decisions. Understanding an organization’s cybersecurity risk profile could also validate whether their current security measures and controls are implemented and working properly or identify gaps and areas of improvement.

2) **Item 106(b)(ii):** “The registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program [and a description of the class of services and solutions those third parties are providing].”

We recommend Item 106(b)(ii) also require the registrant to disclose the services and solutions provided by third parties. This information will provide investors access to important information about the registrant’s cybersecurity risk assessment program they may not otherwise have access to in order to make informed investment decisions.

Tenable believes Item 106(b) and (c) with Tenable’s proposed changes support the intent of the proposed rule to provide “decision-useful information” concerning “whether and how a registrant is managing cybersecurity risks [which] could impact an investor’s return on investment.”

**Question 21.** As proposed, a registrant that has not established any cybersecurity policies or procedures would not have to explicitly state that this is the case. If applicable, should a registrant have to explicitly state that it has not established any cybersecurity policies and procedures?

Yes. A registrant should have to explicitly state if they have not established any cybersecurity policies and procedures. As stated above, cybersecurity breaches can damage a company’s financial condition. In addition to the
costs of remediation from a cyberattack and loss of customers, revenue and reputation, there are risks of loss of proprietary information, shareholder lawsuits, customer lawsuits, increases in insurance premiums and increased scrutiny from external auditors and regulators, among other things.

There are indirect consequences to cyber failures as well; cyberattacks can distract management and divert resources, resulting in new problems unrelated to the breach; they can also trigger customer audits of a company’s cybersecurity defenses, which can lead to the involvement of outside counsel and other third parties, and significant added expenses. If an organization does not have adequate cybersecurity controls and defenses, shareholders have a right to know and factor in that risk to their investment decisions.

**Question 22.** Are there concerns that certain disclosures required under Item 106 would have the potential effect of undermining a registrant’s cybersecurity defense efforts or have other potentially adverse effects by highlighting a registrant’s lack of policies and procedures related to cybersecurity? If so, how should we address these concerns while balancing investor need for a sufficient description of a registrant’s policies and procedures for purposes of their investment decisions?

In general, Tenable believes that the disclosures specified in Item 106 regarding a registrant’s policies and procedures, if any, for identifying and managing cybersecurity risks, a registrant’s cybersecurity governance, including the board of directors’ oversight role regarding cybersecurity risks, and management’s role and relevant expertise in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies would be beneficial in promoting transparency.

Additionally, this transparency should provide an incentive for the registrant to develop, implement, and maintain cybersecurity governance, policies and procedures in line with industry best practices and standards.
However, per Item 106(b)(vi), Tenable believes registrants should only be required to disclose at a high-level whether “[p]revious cybersecurity incidents informed changes in the registrant’s governance, policies and procedures, or technologies.” Requiring the disclosure of specific details about how registrants are changing their programs in response to breaches to protect their enterprise could undermine the cybersecurity defenses of the registrant and make the registrant more vulnerable to cyberattacks.

Tenable does not believe other disclosures required under Item 106 would undermine a registrants’ cybersecurity defense efforts. While there may be incremental risks associated with a registrant’s disclosures regarding their lack of policies and procedures related to cybersecurity, we feel the risk to the registrant is outweighed by the risk to a potential investor who is not able to assess a registrant’s cybersecurity policies and procedures.

Question 23. Should we exempt certain categories of registrants from proposed Item 106, such as smaller reporting companies, emerging growth companies, or FPIs? If so, which ones and why? How would any exemption impact investor assessments and comparisons of the cybersecurity risks of registrants? Alternatively, should we provide for scaled disclosure requirements by any of these categories of registrants, and if so, how?

We do not think the SEC should exempt any categories of registrants from proposed Item 106(b), including smaller reporting companies, emerging growth companies, or FPIs. All organizations are potential targets of threat actors, who typically cast a wide net and are indiscriminate in their threat activities. Further, it is often smaller organizations that have implemented the weakest cybersecurity defenses and are least mature in their basic cyber hygiene protections, such as regularly patching software, ensuring devices are properly configured, using multi-factor authentication and enforcing least privileges to systems and data. Increased transparency with respect to companies’ cybersecurity risk management is valuable to
investors when making investment decisions, regardless of filer type.

**Question 24.** Should we provide for delayed compliance or other transition provisions for proposed Item 106 for certain categories of registrants, such as smaller reporting companies, emerging growth companies, FPIs, or ABS issuers? Proposed Item 106(b), which would require companies to provide disclosures regarding existing policies and procedures for the identification and management of cybersecurity incidents, would be required in annual reports. Should the proposed Item 106(b) disclosures also be required in registration statements under the Securities Act and the Exchange Act?

We do not think the SEC should significantly delay compliance with Item 106, but instead provide for a period of transition for compliance. Cybersecurity risk assessment programs should be a foundational and strategic function of all organizations, no matter the age, size or industry. A decision to delay compliance would signal that cybersecurity risk assessment is only relevant to specific segments of companies, when the reality is that all organizations are potential targets by threat actors. It is to the benefit of companies, their customers and their shareholders to ensure that adequate cybersecurity controls and defenses are implemented without exception or the ability to delay compliance due to a technicality.

**Question 25.** To what extent would disclosure under proposed Item 106 overlap with disclosure required under Item 407(h) of Regulation S-K ("Board leadership structure and role in oversight") with respect to board oversight of cybersecurity risks? To the extent there is significant overlap, should we expressly provide for the use of hyperlinks or cross-references in Item 106? Are there other approaches that would effectively decrease duplicative disclosure without being cumbersome for investors?

We do not think disclosure under proposed Item 106 overlaps with disclosure required under Item 407(h) with respect to board oversight of cybersecurity risks. Rather, the two disclosure requirements would supplement each other. Item
407(h) of Regulation S-K focuses on board governance generally, while certain proposed disclosure in Item 106 focuses on board governance with regard to cybersecurity. If registrants are allowed to hyperlink or cross-reference to their 407(h) disclosure, it will place less emphasis on cybersecurity and counter the intent of the proposed rule. In addition, registrants might take that opportunity to provide less detail on their cybersecurity governance policies than is intended by the proposed rule.

While board oversight of cyber risks is only one piece of proposed Item 106, it is an important one. Allowing cross-references could relegate cyber oversight to a laundry list disclosure of the board’s oversight function generally without giving investors the detailed information they need to understand if a board is educated and engaged on cyber risk.

Tenable hopes that this input will be helpful to the SEC in highlighting the elements of the proposed rule that we believe should be modified or left intact to achieve the SEC’s stated goals, while becoming more consistent with cybersecurity standards and best practices, especially as they relate to cybersecurity policies and practices.

Thank you for your time and consideration. Should you have any questions, or if we can assist in any other way, please let us know.

Sincerely,

Amit Yoran
Chairman and CEO
Tenable, Inc.