SAFE

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

Date: Sept 7th 2022

Ms. Countryman,

Safe Securities Inc. is pleased to respond to the Securities and Exchange Commission (SEC or Commission) request for comment on its proposed rules, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

We support the Commission's objective of enhancing and standardizing disclosures that registrants make about cybersecurity incidents and their cybersecurity risk management, strategy and governance.

Cybersecurity threats present a critical risk to shareholders and more broadly, our macroeconomic environment. We applaud the Commission's efforts to set up a framework to improve the disclosures about material cybersecurity incidents and a robust cybersecurity risk management plan.

We offer the following observations and recommendations on the proposal.

Request for comment #17: 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?

Observations: We recommend adding the following aspects:

1. **How does the organization quantifiably understand and measureably improve their cyber risk posture over time?** An organization should have a consistent risk quantification methodology that incorporates governance across people, processes and technology, taking into account signals from across the tech stack - from Public (and private cloud), SaaS and On-Prom Assets to make up the organization wide risk posture. An organization should invest to build resilience by testing real time ability to remain within an accepted risk level.

2. **How does the organization monitor its attack surface and open gaps on a real time basis?** In an ever changing threat environment, visibility of internal controls is key to predict and prepare. As attack surfaces are getting more complex, it is easy to miss control gaps in your environment. These gaps can be then exploited by attackers. Real-

time visibility of these gaps is critical to manage one's cyber health.

3. **How does the organization prioritize its cybersecurity investments and risk management plan?** With limited investment budgets, security teams will have to always prioritize their actions. How does the security team prioritize? Is it generally based on intuition, or subjective inputs, or quantitative methods to maximize risk reduction? How does the security team take the requirements of different business unit owners into account for prioritization? Our experience shows that quantitative methods (such as bayesian analysis, Monte Carlo Simulations etc) that translate technical risk into business risk effectively, are the most effective in prioritizing.

4. **How does the organization understand cyber risk by different applications, business units and business locations?** With globally distributed companies with multiple applications processing (and storing) customer data, it is important to understand cyber risk by different applications, business units and locations of operations. For example, in a financial services company, the retail banking unit might have a different type of exposure compared to the investment banking unit. And accordingly, the risk management plan will be different. Similarly business locations expose companies to specific country regulations and risk factors.

5. **How does the organization test its incident response and business continuity plans?** Having these plans is not enough. Are those plans regularly stress tested? What is the frequency of testing? How are the plans improved regularly?

Request for comment #26: Would proposed Item 407(j) disclosure provide information that investors would find useful? Should it be modified in any way?

Observations: We recommend to add the following:

1. Boards should ask for an objective visibility of inherent risk and residual risk after taking into account all risk mitigation and transfer controls being applied?
2. How frequently does the board interact with the IT and the Security team?
3. Does the board (or risk or the audit committee) have tabletop exercises with the IT and the Security team on cyber risk management?
4. How does the board translate the cyber risk into risk to shareholders' value?
5. Boards should also question the Return on Security Investment (ROSI)?
6. Does the board sign off on the final acceptable residual risk?

Request for comment #27: Should we require disclosure of the names of persons with cybersecurity expertise on the board of directors, as currently proposed in Item 407(j)(1)? Would

a requirement to name such persons have the unintended effect of deterring persons with this expertise from serving on a board of directors?

Observations: We recommend that it should not be required to disclose the names of persons with cybersecurity expertise on the board of directors. In addition to the unintended effect mentioned, we believe that the entire board should take joint responsibility for a robust cybersecurity risk management plan, not just an individual board member.

We would welcome an opportunity to discuss our comments in a meeting.

Sincerely

Saket Modi
CEO and Co-Founder
Safe Security

Email : [redacted]
Website : www.safe.security