The Institute of Internal Auditors
Elevating Impact

May 9, 2022

Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Dear Chairman Gensler and Commissioners Peirce, Lee, and Crenshaw:

The Institute of Internal Auditors (IIA) thanks the Securities and Exchange Commission (SEC) for the opportunity to share comments on your pending Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proposal.

For over 80 years, The IIA and its now more than 210,000 members across the globe have aided sound governance and risk management efforts in public- and private-sector organizations, encouraging strong internal controls and an enterprise-wide approach. Auditing information systems and security is top of mind for practitioners and policymakers in this age of digital transformation and disruption, and we know from The IIA's OnRisk 2022 survey that cybersecurity remains a top risk identified by chief audit executives, boards of directors, and C-suite executives.

The IIA recognizes that certain disclosures of an organization's cybersecurity risk management, strategy, governance, and material incidents can be useful information for investors and other stakeholders and commends your efforts to examine these topics.

In response to your request for comments, we offer the following feedback and suggestions.

Conceptual Model for Governance, Risk Management, and Internal Controls

The IIA believes that the SEC would benefit from explicitly recognizing and aligning its proposal with The IIA's Three Lines Model, widely recognized globally as a critical resource in successful governance. The model helps organizations identify roles and responsibilities for setting strategies and objectives, managing risks – including cyber risks – and delivering benefits and information to stakeholders. The model establishes the three essential functions of governance as:

- Accountability of a governing body to stakeholders for organizational oversight through integrity, leadership, and transparency.
- Actions (including managing risk) by management to achieve the objectives of the organization through risk-based decision-making and application of resources.

- Assurance and advice by an objective, independent internal audit function to promote trust among stakeholders and continuous improvement through rigorous inquiry and insightful communication.

The Three Lines Model provides a foundation for describing the roles and responsibilities of the governing body, management, and independent assurance providers in setting strategies, assessing risks, designing and implementing controls, and providing assurance to stakeholders that governance, risk management, and control processes are adequately ensuring the achievement of objectives. This model is well-suited to ensuring that the organization's objectives for cybersecurity are met while mitigating potential disruptions from cyberattacks. In this way, an independent assurance function is fundamental to supporting mutual trust among stakeholders.

The IIA's International Standards for the Professional Practice of Internal Auditing (The IIA *Standards*)

The IIA *Standards* establish a framework for governing and managing an internal audit function, which can provide valuable assurance and advisory services, including engagements covering cybersecurity risks. The *Standards*, together with recommended guidance, represent best practices for assessing the design and implementation of processes for governing and managing cybersecurity controls, including those that ensure compliance with SEC reporting requirements. We believe the SEC should consider requiring registrants to report whether their internal audit activity conforms with the IIA *Standards*.

Holistic Approach to Governance and Risk Management

The IIA, as a founding and supporting member of the Committee of Sponsoring Organizations (COSO), wants to emphasize the importance of positioning cybersecurity risks as components of an organization's overall governance and enterprise risk management (ERM) processes, versus establishing siloed governance and risk management functions dedicated solely to cybersecurity in general, or regulatory reporting requirements in particular.

Responses to Specific Requests for Comment

Request #20: Should we require the registrant to specify whether any cybersecurity assessor, consultant, auditor, or other service that it relies on is through an internal function or through an external third-party service provider? Would such a disclosure be useful for investors?

IIA Response: It is likely that a significant majority – possibly the entirety – of SEC registrants employ both internal and external resources for assurance and consulting services regarding cybersecurity risks and controls. For example, second-line management functions such as ERM, information security, and compliance, as well as the third-line internal audit activity, often provide cybersecurity risk assessments and control advice using a mix of internal and external resources. Therefore, we do not believe that it would be particularly useful to stakeholders for a registrant to simply state as much. Rather, we believe what would benefit stakeholders more would be an appropriately positioned, funded, and skilled internal audit function providing independent assurance that the organization employs effective, enterprise-wide approaches to cybersecurity governance and risk management. Additionally, internal audit can provide uniquely relevant advice and consulting, including the evaluation of opportunities for improving cybersecurity processes, given its familiarity with the organization.

Request #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?

IIA Response: While The IIA appreciates the goal of providing decision-useful information to investors, we are not convinced that this proposal would necessarily achieve that objective. The SEC's comment on p. 69 "given the level of the specificity that would be required, the resulting disclosures are unlikely to become boilerplate," seems to be in conflict with the statement on p. 21 "we would not expect a registrant to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." Indeed, we believe that such disclosures would tend to end up in a boilerplate format.

As an alternative to disclosing cybersecurity policies, procedures, and governance as currently proposed, we suggest that a more useful approach to ensuring cyber incidents are managed and reported effectively might be to require registrants to disclose whether they fully adopt or participate in law enforcement or national security programs, such as the Shields Up program from the Cybersecurity and Infrastructure Security Agency.

Request #1: Would investors benefit from current reporting about material cybersecurity incidents on Form 8-K? Does the proposed Form 8-K disclosure requirement appropriately balance the informational needs of investors and the reporting burdens on registrants?

IIA Response: For the first question, The IIA supports the SEC's role in protecting investors' interests and the objective of requiring disclosures of material events in a timely fashion. For financial reporting, the concept of materiality is time-tested, even though it is defined as including

objective and subjective measures. For non-financial reporting, especially for relatively new types of events such as cyber incidents and data privacy breaches, established norms for determining materiality have not yet been widely adopted, as illustrated by the current proposal's lack of guidance for determining the materiality of cyber incidents. For this reason, The IIA believes that focusing on the timeliness aspect of material cyber incident reporting misses the bigger question, one which may underlie the conundrum noted by the SEC staff in discrepancies between cyber incident reporting on 8-K and 10-K forms – how and when should an organization determine the materiality of a cyber incident? Therefore, we believe the SEC should provide clearer guidance in this area concurrent with, if not before, implementing a four-day disclosure requirement.

Request #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?

IIA Response: On p. 60, the SEC indicates that the average affected filer had total assets of $14.1 billion and a market capitalization of $5.6 billion in 2020. While we would not oppose this proposal, per se, we believe it is highly unlikely that any SEC registrants would not have "established any cybersecurity policies or procedures." Therefore, we recommend that the SEC focus on ensuring that those cybersecurity policies and procedures are tested, and their effectiveness validated through a properly resourced and positioned independent assurance function. Doing so will enhance the trust that all stakeholders can have in the information they are given regarding the organization's management of cybersecurity risks and the occurrence and impact of cyberattacks.

Request #38: Should we amend Form 20-F, as proposed to require disclosure regarding cybersecurity risk management and strategy, governance, and incidents? Additionally, should we amend Form 6-K, as proposed, to add "cybersecurity incidents" as a reporting topic? Are there unique considerations with respect to FPIs in these contexts?

IIA Response: For the Form 20-F amendments, which would require foreign private issuers (FPIs) to disclose the same information as Items 106(b) and (c) of Regulation S-K [see Request #17] would require for domestic registrants, The IIA's response is the same as to request #17. In short, disclosures of the existence of policies and procedures are not as beneficial to stakeholders as the implementation of a well-designed system of checks and balances to ensure an organization's strategic, operational, reporting, and compliance objectives are achieved.

For the Form 6-K amendments, which would ask FPIs to report cybersecurity incidents the same as proposed changes to Form 8-K for domestic registrants, The IIA's response is the same as to request #1. In short, the SEC should develop guidance for determining the materiality of a cyber incident before or concurrent with implementing a four-day disclosure requirement.

Request #43: Would both types of the proposed disclosure, cybersecurity incident disclosure and cybersecurity risk management, strategy, and governance disclosure, increase the vulnerability of registrants to cybersecurity incidents? Would this effect be mitigated by any of the other effects of the proposal, including indirect effects such as registrants' potential strengthening of cybersecurity risk management measures? What would be the impact of the proposed disclosure on the likelihood of future incidents for registrants? Would that impact be the same for both types of disclosure?

IIA Response: Similar to our response to request #17, The IIA expects that SEC registrants would prefer to keep the details of cybersecurity risks and controls confidential. Furthermore, it is uncertain whether such reporting requirements ultimately agreed to would result in increased vulnerability for the registrants. As stated before, The IIA's position is that the best way to manage an organization's unique cyber risks is to: align processes with widely adopted guidance; actively participate in law enforcement efforts that can strengthen the control environment for all stakeholders; and support those efforts with independent internal assurance that conforms with the IIA *Standards*.

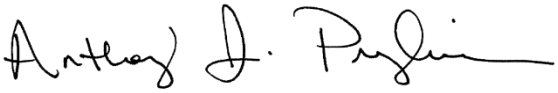
Request #19: The proposed rule does not define "cybersecurity." We could define the term to mean, for example: "any action, step, or measure to detect, prevent, deter, mitigate, or address any cybersecurity threat or any potential cybersecurity threat." Would defining "cybersecurity" in proposed Item 106(a) be helpful? Why or why not? If defining this term would be helpful, is the definition provided above appropriate, or is there another definition that would better define "cybersecurity"?

IIA Response: The IIA would support efforts by the SEC to standardize definitions of "cybersecurity", as long as the Commission works closely with the National Institute of Standards and Technology, the Cybersecurity and Infrastructure Security Agency, the Office of the National Cyber Director, and other relevant departments and agencies to ensure government-wide consistency.

The Institute of
Internal Auditors
Elevating Impact

Thank you for your consideration of our comments. The IIA offers our ongoing assistance to support your development of the Commission's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proposal. Please do not hesitate to contact me or Vice President of Global Advocacy, Policy, and Government Affairs, Mat Young, (mat.young@theiia.org, (202) 270-0170), for any questions, comments, or additional input.

Sincerely,



Anthony J. Pugliese, CIA, CPA, CGMA, CITP
President and Chief Executive Officer
The Institute of Internal Auditors, Global Headquarters