Cybersecurity Coalition

May 9, 2022
Via e-mail: rule-comment@sec.gov
Vanessa Countryman, Secretary
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:

The Cybersecurity Coalition ("Coalition") submits these comments in response to the proposed rule issued by the Securities and Exchange Commission ("SEC"). The Coalition appreciates the opportunity to comment on the SEC's *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* proposal, and believes that the commentary offered will be helpful to the SEC in understanding the cybersecurity industry's perspective on several key elements of the proposed amendments.

The Coalition is composed of leading companies specializing in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[1] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community. Many Coalition members are publicly traded.

In general, the Coalition is supportive of the effort being put forward and the issues it seeks to address. The Coalition is also appreciative of the former SEC interpretive guidance on disclosure obligations related to cybersecurity risks, and would recommend an approach that can maintain consistency with such guidance. However, several areas that suggest a slightly more prescriptive approach to reporting can present cyber risk, and we identified these concerns below.

As an additional resource, the Coalition is pleased to provide the SEC with an overview of our prior position underlining several key principles for cyber incident reporting regimes. These

[1] The views expressed in this comment reflect the consensus views of the Coalition, and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org

principles are generally reflected in the recently passed "Cyber Incident Reporting for Critical Infrastructure Act of 2022" ("CIRCIA"). They include:

- Establishing feasible reporting timelines of no less than 72 hours of determination of a significant or material incident[2] for reporting incident information *in confidence*, while allowing for supplemental reporting as more information becomes known.
- Limiting reporting to verified incidents
- Limiting reporting obligations to the victim organization rather than third parties
- Harmonizing federal cybersecurity incident reporting requirements
- Ensuring confidentiality and nondisclosure of incident information provided to the government
- Balancing the urgency to notify with the need to provide accurate information
- Reporting should complement, not compete with, the incident response procedures of victim entities, or otherwise subject victim entities to additional risk.

Detailed below are the Coalition's responses to specific questions as numbered within the proposed rule.

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?

A) The Coalition believes that cybersecurity is increasingly important to investors and business operations. Current reporting about material cybersecurity incidents may provide additional transparency to investors regarding the registrants' cyber resiliency, and effects of the incident on finances and operations. However, requiring registrants to publicly disclose incidents prior to remediation of the incident may undermine cybersecurity, and creates risks to companies, investors, and consumers. We detail these concerns below.

2. Would proposed Item 1.05 require an appropriate level of disclosure about a material cybersecurity incident? Would the proposed disclosures allow investors to understand the nature of the incident and its potential impact on the registrant, and make an informed investment decision? Should we modify or eliminate any of the specified disclosure items in proposed Item 1.05? Is there any additional information about a material cybersecurity incident that Item 1.05 should require?

A) In general, the Coalition has significant reservations about Item 1.05 requiring that registrants' incident disclosures address specifically whether an incident is ongoing

[2] 72-hours represents the minimum amount of time that is required for a victim to report an incident in the context of the CIRCIA (certain incident information which is reported in confidence). The Coalition acknowledges that collecting sufficient and complete information to conduct the materiality assessment can entail a longer timeline which start may commence after the remediation is concluded. We expand on the issue below. This is important, since determinations conducted in premature stages may result in providing misleading, inaccurate, or not useful information that puts other parties at risk – given the nature of this information.

and whether an incident has been remediated. The Coalition appreciates the SEC's acknowledgment that registrants are not expected to disclose specific technical information "in such detail as would impede the registrant's response or remediation of the incident," but the Coalition is nevertheless concerned that requiring a public acknowledgment that an incident is ongoing and less-than-fully remediated would be contrary to cybersecurity best practices, and may put SEC registrants and their investors – and the ecosystem and nation at large - at unnecessary additional risk.

Accordingly, the Coalition believes the proposed Item 1.05 disclosures should be refined to promote security interests while still providing necessary transparency to investors. Ideally, and in accordance with long established cybersecurity best practices, limited (if any) information should be publicly disclosed about incidents that have yet to be remediated. There are a few specific exceptions to this principle, but the Coalition believes the SEC's disclosure rule should adhere to this best practice.

In any event, the Coalition emphatically supports the removal of any requirement to specifically disclose an incident's remediation status on Form 8-K. Rather, the rule should permit registrants flexibility to determine the level of specificity that is appropriate for public consumption in light of active security risks, and to withhold certain details (such as the incomplete status of remediation), or perhaps delay detailed disclosure altogether, if the registrant reasonably believed disclosure of certain details would exacerbate the material impact of the incident.

3. Could any of the proposed Item 1.05 disclosures, or the proposed timing of the disclosures have the unintentional effect of putting registrants at additional risk of future cybersecurity incidents? If so, how could we modify the proposal to avoid this effect? For example, should registrants instead provide some of the disclosures in proposed Item 1.05 in the registrant's next periodic report? If so, which disclosures?

A) The Coalition generally supports the SEC's goal to inform investors of material cybersecurity incidents in a consistent and timely manner. The Coalition also applauds that the SEC's proposed rule states that disclosures need not disclose specific technical information that would impede cybersecurity activities like incident response.[3]

However, while disclosure of a *remediated* cyber incident is possible four days after a materiality determination, disclosure of an ongoing cyber incident creates new risks. As noted above, the Coalition is against any mandatory public revelations about incidents that are ongoing, or where remediation efforts are incomplete. This would be against established best practices, and has the potential to worsen a cybersecurity incident for both the victim registrant and investors.

[3] Pg. 21. "While registrants should provide disclosure responsive to the enumerated items to the extent known at the time of filing of the Form 8-K, 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."

Requiring detailed disclosure on a current basis on Form 8-K may result in registrants revealing the existence of a cybersecurity incident before such incident is fully mitigated or remediated, and the impacted information system fortified against similar threats. In addition, the proposed rule would require a registrant to disclose whether or not the incident has been remediated, which has the effect of calling out the status of the registrant's ability to remediate the incident at a time when the registrant is at its most vulnerable state. The nature of the proposed current reporting could unintentionally invite additional threat actors to take advantage of the vulnerability, resulting in additional harm to registrants and their investors. In most cases, if a registrant experiences a cybersecurity incident, it is in the best interests of the registrant and its investors for the registrant to focus on identifying and remediating the incident prior to public disclosure of the incident.

Finding the appropriate balance between cybersecurity and transparency is a difficult problem that may not have an elegant solution. However, the SEC should consider possible options for modifying its proposal to avoid creating additional risks. This may include permitting registrants to delay the filing of Form 8-K concerning a material cybersecurity incident until it has been remediated. Circumstances that could justify such delay include where the registrant is actively pursuing timely mitigation of the incident, but cannot reasonably complete that process within four days of a materiality determination, and the registrant reasonably believes public disclosure of the incident prior to mitigation would exacerbate the material impact of the incident.

If the SEC maintains that current, detailed reporting is required in all cases, then 8-K disclosures on cybersecurity incidents should not require the disclosure of the status of mitigation or remediation, and registrants should be afforded significant latitude as to the substance and detail of such disclosures, to minimize the risk to the registrant and investors alike. Registrants should not be required or advised to report specifics of unmitigated vulnerabilities or ongoing cybersecurity incidents.

4. We are proposing to require registrants to file an Item 1.05 Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident. Would the proposed four-business day filing deadline provide sufficient time for registrants to prepare the disclosures that would be required under proposed Item 1.05? Should we modify the timeframe in which a registrant must file a Form 8-K under proposed Item 1.05? If so, what timeframe would be more appropriate for making these disclosures?

A) To the extent Form 8-K reporting is required, the Coalition believes that the four-business day filing deadline from the point that a registrant determines that it has experienced a material cybersecurity incident is adequate for incidents that have been remediated as it is consistent with global best practices. At a minimum, registrants should never be required to report sooner than 72 hours after a covered incident is confirmed. This timeframe is reflected in numerous national and international reporting regimes such as the European Union's (EU) *General Data Protection Regulation* (GDPR), New York

State's (NYS) *Part 500 Cybersecurity Requirements for Financial Services Companies* (23 CRR-NY 500), The Australian *Security Legislation Amendment (Critical Infrastructure) Act 2021*, and others.[4, 5, 6]

Remediated cyber incidents may be appropriately disclosed under Form 8-K within four days of the materiality determination, but registrants should be provided additional time to remediate the incident before public disclosure if necessary. While registrants may be capable of preparing the disclosure within four-business days, the Coalition has concerns that the public disclosure of a yet-to-be remediated cyber incident will create new cybersecurity risks for registrants and investors. Our concerns and proposed alternatives are detailed above.

It should also be noted that cybersecurity incidents affecting registrants may become public through the press or other third parties when no 8-K has been filed, and any such mismatch between newsworthiness and materiality is neither unexpected nor unique to cybersecurity matters. For example, there may be incidents that the press or other third parties deem "significant" or otherwise of interest for a variety of reasons, but that the registrant has reasonably determined does not meet the materiality threshold for investors at the time, or possibly ever. The SEC should not expect or conclude that press or other third-party statements about cybersecurity incidents, which could be unsubstantiated and based on speculation rather than fact, create a presumption that a Form 8-K will be filed. Form 8-Ks will not necessarily match the public record for cybersecurity incidents, and such a mismatch should not be considered indicative of a registrant failing its reporting obligations.

5. Should there be a different triggering event for the Item 1.05 disclosure, such as the registrant's discovery that it has experienced a cybersecurity incident, even if the registrant has not yet been able to determine the materiality of the incident? If so, which information should be disclosed in Form 8-K based on a revised triggering event? Should we instead require disclosure only if the expected costs arising from a cybersecurity incident exceed a certain quantifiable threshold, e.g., a percentage of the company's assets, equity, revenues or net income or alternatively a precise number? If so, what would be an appropriate threshold?

A) The Coalition is supportive of the SEC's proposal to define the triggering event for any required non-periodic reporting as "the date on which a registrant determines that a cybersecurity incident it has experienced is material."[7] This definition aligns with the principle of balancing the urgency of submitting an incident notification with the need for accurately assessing an incident's significance.

[4] https://gdpr-info.eu/
[5] https://www.governor ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf
[6] https://www.legislation.gov.au/Details/C2021A00124
[7] https://www.sec.gov/rules/proposed/2022/33-11038.pdf

Public disclosure of cybersecurity incidents before a materiality determination has been made risks needlessly confusing investors by inundating them with reports of cybersecurity incidents that are later assessed to have had no meaningful impact. The additional reports that would be created by earlier disclosures would likely misrepresent the quantity and significance of cybersecurity incidents to investors in a way that would hinder their ability to make informed decisions and potentially cause investor under- or over-reactions that may result in mispricing of securities.

In relation to significance, the Coalition supports the use of the materiality standard. The materiality standard is a well-established concept that is familiar to SEC registrants and it provides adequate flexibility for assessing various types of cyber-related incidents. We would recommend against creating a new standard for cybersecurity incidents that is distinct from the materiality standard used for other required disclosures. It is not clear that "expected costs" or any other threshold or methodology would be more consistent or easier to apply.

6. To what extent, if any, would the proposed Form 8-K incident reporting obligation create conflicts for a registrant with respect to other obligations of the registrant under federal or state law? How would any such conflicting obligations arise, and what mechanisms could the Commission use to ensure that registrants can comply with other laws and regulations while providing these timely disclosures to investors? What costs would registrants face in determining the extent of a potential conflict?

A) The Coalition is aware of the growing number of disparate federal and state cyber incident reporting regimes, including the recent CIRCIA. Variations among cyber incident reporting regimes strain organizations who must ensure they comply with different definitions of covered incidents, reporting timelines, reporting content requirements, reporting formats, and more. That is in addition to the deconfliction process of understanding how various cyber incident reporting regimes affect an organization's obligation to other laws and regulations.

This is why the Coalition supported the recent CIRCIA's creation of a Cyber Incident Reporting Council "to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations."[8]

The Coalition is not in the position to outline how all the various combinations of reporting regimes may create conflicts for registrants. However, the Coalition strongly urges the harmonization of these cyber incident reporting regimes where possible, and encourages the SEC to assess existing regimes, and to work with the Cyber Incident Reporting Council to maximize alignment. This is true in particular where requirements can be in direct conflict (e.g., disclose information to the public at large, compared to maintaining it in confidence, as required by security best practices).

[8] https://www.congress.gov/117/bills/hr2471/BILLS-117hr2471enr.pdf

7. Should any rule provide that the Commission shall allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security?

A) The Coalition believes the Attorney General, or their designee, should have the ability to request a delay in reporting a cybersecurity incident in the interest of national security. Any cybersecurity incident that rises to the level of national security concern would plausibly put investors at far greater risk if disclosed than if investors were delayed in receiving a cybersecurity incident disclosure. In such instances, the security of the nation and of all investors should be prioritized.

8. We are proposing to include an instruction that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." Is this instruction sufficient to mitigate the risk of a registrant delaying a materiality determination? Should we consider further guidance regarding the timing of a materiality determination? Should we, for example, suggest examples of timeframes that would (or would not), in most circumstances, be considered prompt?

A) The Coalition is supportive of a flexible instruction to make a materiality determination as soon as reasonably practicable after discovery of the incident. We caution against imposing a specific timeframe on the materiality determination, because of the high degree of variability in cybersecurity incidents. Each cybersecurity incident is unique and the number of variables that impact the materiality calculus does not lend itself to a more defined approach. As the Coalition stated in the principles above, the urgency to report must be balanced with the need for accuracy, and reporting should complement, not compete with, the registrant's incident response activities.

Each registrant's combination of systems, structure, policies and procedures, cybersecurity maturity, line of business, and available resources is unique, and each will affect the speed at which a cybersecurity incident's materiality can be determined. Likewise, the type and sophistication of a cybersecurity incident can vary greatly and may add significant complexity to the determination process.

Providing further guidance and suggested timeframes risk registrants feeling obligated to adjust response procedures to make a determination to the detriment of remediation efforts. Such an outcome would represent additional risk to the registrant and its investors. Additionally, such guidance may lead registrants to report when they have insufficient evidence to make an accurate judgment on the materiality of a cybersecurity incident. This may lead to overreporting of non-material cybersecurity incidents or lead to underreporting of material cybersecurity incidents. Furthermore, it risks creating unrealistic expectations for investors who may feel deceived or misled when incident reporting falls outside of the guidance or examples provided by the SEC. It is in the best

interest of the registrant and investors for the registrant to follow best practices to identify and remediate the incident and not make a premature materiality determination.

10. As described further below, we are proposing to define cybersecurity incident to include an unauthorized occurrence on or through a registrant's "information systems," which is proposed to include "information resources owned or used by the registrant." Would registrants be reasonably able to obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them? Would a safe harbor for information about cybersecurity incidents affecting information resources that are used but not owned by a registrant be appropriate? If so, why, and what would be the appropriate scope of a safe harbor? What alternative disclosure requirements would provide investors with information about cybersecurity incidents and risks that affect registrants via information systems owned by third parties?

A) The Coalition strongly opposes the notion that the definition of "cybersecurity incident" should cover anything other than a registrant's own information systems. This is in line with the principle that third-party reporting should be avoided. While registrants may have some visibility into a cybersecurity incident that affects information resources, they use but do not own, only the owner of the information system itself is in a position to assess the full implications of the incident. This is especially true for complex cloud environments.

A specific concern is the inclusion of "used by" in relation to the proposed definition of "information systems", which risks inaccurate disclosures due to a registrant's lack of information or knowledge concerning an incident. This may create confusion for investors about the nature of an incident. Furthermore, it may introduce friction and distrust between registrants and their IT vendors, to the detriment of investors. The Coalition recommends replacing "used by" with "operated by" within the proposed definition.

14. Should we include Item 1.05, as proposed, in the list of Form 8-K items where failure to timely file a Form 8-K will not result in the loss of a registrant's eligibility to file a registration statement on Form S-3 and Form SF-3?

A) The Coalition agrees with the SEC's view that a failure to timely file a Form 8-K should not result in the loss of a registrant's S-3 eligibility. Given the complexity surrounding cybersecurity detecting, analyzing, and remediating cybersecurity incidents (including as to materiality determination), and the harsh consequences to a registrant from losing S-3 eligibility, it is not in the best interests of investors for a registrant to lose S-3 eligibility.

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?

A) The Coalition recommends the SEC replace item 106(b)(1)(i) with the following:

- The registrant has a cybersecurity risk assessment program and, if so, whether it uses best practices and standards to identify and protect against cybersecurity risks and to detect and respond to cybersecurity events, and if not provide a description of the program.

The Coalition believes it would be useful for investors to know whether the registrant's risk assessment program follows risk management best practices and standards to control or mitigate risks. If a registrant is not following an established set of best practices and standards, then the registrant should describe the nature of their cybersecurity program.

The Coalition believes Item 106(b) and (c), and this proposed change supports 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."

18. Are the proposed definitions of the terms "cybersecurity incident," "cybersecurity threat," and "information systems," in Item 106(a) appropriate or should they be revised? Are there other terms used in the proposed amendments that we should define?

A) As reflected in our response to question 10, the Coalition feels the definition of "Information systems" should only include those systems operationally controlled by the registrant. We recommend replacing "used by" with "operated by" within the proposed definition. If the registrant uses a third-party system, they should not be required to report cybersecurity incidents that may occur on such systems. In the event a cybersecurity incident at a third-party provider has a material impact on the registrant, the registrant should report the activity under Item 8.01.

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?

A) The Coalition recommends that a registrant should have to explicitly state if they have not established any cybersecurity policies and procedures. As the proposed rule

highlights, a cybersecurity incident could result in a material impact to a registrant. Consequently, investors have the right to know if a registrant has not established any cybersecurity policies or procedures.

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?

A) The Coalition 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 a cybersecurity incident could undermine the cybersecurity defenses of the registrant and make the registrant more vulnerable to cyberattacks.

The Coalition does not believe that the disclosures required under Item 106 would necessarily undermine a registrants' cybersecurity defense efforts as long as they are sensibly described. 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.

In general, the Coalition 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 to investors on this increasingly important aspect of corporate governance.

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. An approach to consider would be to initiate the Item 106 disclosures after the regulation is finalized to provide registrants time to implement their cybersecurity policies and procedures.

The Coalition does, however, recommend that the SEC revise its proposed amendments to Item 106(d) to clarify that a registrant need only provide updates to "previously disclosed material cybersecurity incidents," and need not make disclosures relating to immaterial incidents (unless they have become material in the aggregate, as proposed) that may have been addressed in the press or other third-party reports.

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?

A) The Coalition does not believe 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. Increased transparency with respect to companies' cybersecurity risk management is valuable to investors when making investment decisions, regardless of filer type.

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 asset-backed securities 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?

A) The Coalition does not think the SEC should significantly delay compliance with Item 106, but may 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.

The Coalition hopes that its input will be helpful to the SEC in highlighting the elements of the proposed rule that should be reconsidered or modified to better achieve the SEC's stated goals, while becoming more consistent with cybersecurity standards and best practices, especially as they relate to incident reporting.

Thank you for your time and consideration. Should you have any questions, or if we can assist in any other way, please contact Grant Schneider at [redacted].

Respectfully Submitted,

The Cybersecurity Coalition