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

May 9, 2022  


Dear Secretary Countryman:  


Our response to specific SEC questions are below.  

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?  

Reports on material cybersecurity incidents will help investors more accurately define the inherent operational risks of a company to make more informed investment and voting choices. The proposed disclosure content is practicable for most/all large enterprises, when basic cybersecurity policies and procedures are in place. The timing requirement is perhaps both onerous to the firm and possibly counterproductive to the investor consuming the information, however, as it often requires a security team multiple weeks to fully assess the severity, impact and scope of an incident, especially in larger enterprises. A competent security function operating in a defined policy and procedural framework should have an initial “situational awareness” of an incident’s severity and impact within 3-5 working days, but additional time may be needed to prepare the documentation, perform adequate internal quality and compliance reviews, and solicit subject matter expert opinions and reviews.  

As part of the initial pre-public reporting, law enforcement should be recognized as a consultant. It is not unusual for law enforcement to want incidents to remain out of the media to protect their investigations, and that should be honored.
Entity should at some point also provide comment on long term remediation strategy, so long as no information that can be exploited is revealed. There exists a need to differentiate remediation actions taken during triage versus expected future process, systems, etc. changes to mitigate against similar, potential future incidents.

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?

The requirement “A brief description of the nature and scope of the incident” is less helpful than having a defined severity and impact scoring rubric, along the lines of CVSS v3.0/.1 Ratings [ref: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator], which would allow for aggregate analysis and trend analysis both for a specific company and for comparative analysis across firms and industries. CISA has proposed such a framework here: https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System with a demo prototype here: https://www.cisa.gov/uscert/nciss/demo

A ratings system that would help stakeholders assess the long-term impact to the business makes more sense.

It would be good to see some verbiage around the metrics associated with the incident. How long to identify, how long to contain, how long to mitigate, any associated plan of action to remove/remediate the risk to the company & its investors, so long as it was not sensitive information that might aid attackers. This would allow investors to review the disclosures over time and identify which companies are actually going in the right direction.

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?

We need to minimize the disclosure of anything that would compromise an investigation or would provide intel useful to a hacker. First, there should be an initial, non-public reporting, more like a heads up, to the appropriate governing body, including Law Enforcement. As part of that process, a collaborative decision would be made about what and when should be disclosed.
This could be followed by an interim public report at a later date, and, where appropriate, a final report. Quite often an accurate impact of these incidents is not known for quite some time. Interested parties should be kept abreast as the situation evolves both up and down.

Providing awareness (entity should also disclose additional resources/law enforcement/etc. which are supporting containment/forensics) should encourage investors to maintain awareness to the situation at play, but this also limits the disclosure of information which may: (1) evolve over time, hence reducing retractions or clarifications to comments and disclosures and; (2) introduce additional interest in exploitation of the root of the incident.

Also, appropriate communication is part of the cyber world. Every time a security vulnerability is discovered and/or a patch is released, IT departments all over the world start patching an assessing their infra, that's part of the daily routine from IT. Thus, communication is a key component for everyone’s safety.

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 longer period seems both more realistic and allows for more refined and useful information collection and analysis, without significant negative repercussions for the company, investors, or regulatory reviewers.

An initial, non-public heads up to appropriate government entities, including law enforcement, with something more formal and public to follow makes more sense. Since one of the goals is to improve overall cyber hygiene/ reduce risk, there needs to be Law Enforcement (and potentially other) engagement prior to public disclosure. Deadlines should be tolled at the request of law enforcement IF if both parties agree that it could impede the investigation.

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?

The SEC’s proposed reporting trigger is predicated on the notion that all listed entities must then equally define their view of an incident. Additionally, given the proposed timeline, smaller
organizations may risk reporting false positives, in the event they have lesser resources to promptly make a determination on the incident’s details. The investment community may have knee-jerk reactions upon reading timely incident disclosures. The rule should allow for transparency without creating a sense of panic, and that requires sufficient time for the entity to investigate, gather details with confidence, and report accordingly.

A common practice in security research is to provide for an embargo period after a researcher notifies a company or open source project of an exploitable flaw in code or a product. After that embargo period elapses, regardless of the status of a fix, the researcher is free to release information about the defect publicly. This serves the common good as it gives the project or company a reasonable opportunity to analyze and correct the defect. If the project or company does not provide a fix, the user community is entitled timely warning that an exploitable defect exists in their systems that they may take corrective measures, including discontinuing use of the affected code or component. Otherwise attackers are at an advantage and may independently exploit the defect.

A similar balance exists in the case of incident disclosure, namely that the benefit to a company’s investors of notice of an incident eventually eclipses the potential benefits of non-disclosure after an elapsed period of time. Further, in the case that a firm cannot effectively perform an impact analysis in a reasonable period, so as to determine materiality of the incident, that failure itself implies significant inadequacies of processes, staffing, resources, governance and/or oversight. In these cases, the benefit to the shareholders outweighs any concerns about subsequent attacks or other risks posed by disclosure of the incident.

It would be hard to assign a threshold for reporting, since assigning an accurate estimate of expected cost from the incident is extremely difficult, and there are few rigorously tested and practical or academic methodologies for such accurate estimation, especially where it pertains to loss or compromise of brand equity, consumer and employee goodwill, strategic partnership opportunities, and other intangibles that may subsequently impact a company’s revenues or profits. While vendors and subject matter experts acting as consultants can provide proprietary or untested tools and analysis methods for estimating cost, there has not been sufficient academic or industry research to establish the efficacy of these tools and methods. Federal funding for such research would be highly beneficial to understanding these tools and methods for future consideration.

If the registrant cannot effectively determine the materiality of the incident, the best course of action is to base any threshold on the types and numbers of assets impacted, the attack vectors for the incident, if known, any exposure or loss of customer data, and an accounting of the amount spent to-date as a direct result of the incident. CISA has published incident reporting guidance here: https://www.cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf that should be reviewed and considered. Competent investor analysts can use such data to make their own assessment of materiality.
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?

As discussed above, yes.

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?

Some time pressure is appropriate, since the fact that a registrant cannot effectively perform an impact analysis in a reasonable period, so as to determine materiality of the incident, itself may imply significant inadequacies of processes, staffing, resources, governance and/or oversight. It would be helpful to know what is considered “prompt”, as this may not be entirely straightforward to the investor community. This could also indicate that disclosures exceeding a certain threshold should indicate some dysfunction to the areas of business required to quantify impact (of course, which is of additional concern).

9. Should certain registrants that would be within the scope of the proposed requirements, but that are subject to other cybersecurity-related regulations, or that would be included in the scope of the Commission’s recently-proposed cybersecurity rules for advisers and funds, if adopted, be excluded from the proposed requirements? For example, should the proposed Form 8-K reporting requirements or the other disclosure requirements described in this release, as applicable, exclude business development companies (“BDCs”), or the publicly traded parent of an adviser?

No. We are looking at systemic risk. The percentage of incidents from third party compromises is on the rise.

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 common example of this is cloud computing. In many commercial cloud contracts, there is a definition of a “shared responsibility model” wherein the registrant agrees to accept certain responsibilities, while the cloud provider agrees to maintain specific controls and implement certain requirements for security. However, the choice of using cloud computing, and the particular choice of which cloud vendor or technology to use and how to secure it in relation to the shared responsibility model, ultimately rests on the registrant and is based entirely on a registrant’s particular cost and performance parameters and capabilities. Therefore it is difficult to conceive of a practicable framework for safe harbor that shields registrants from disclosure and materiality analysis, even where the root cause of a given incident is attributed to the cloud provider under the shared responsibility model.

While an organization can transfer responsibility, they are still ultimately accountable to their stakeholders.

11. We are proposing that registrants be required to file rather than permitted to furnish an Item 1.05 Form 8-K. Should we instead permit registrants to furnish an Item 1.05 Form 8-K, such that the Form 8-K would not be subject to liability under Section 18 of the Exchange Act unless the registrant specifically states that the information is to be considered “filed” or incorporates it by reference into a filing under the Securities Act or Exchange Act?

We support the proposal of furnishing the item, not subject to liability under Section 18. Incidents have the ability to evolve over time, and trends/themes of cyber threat intel can shine light on later clarifications or observations to an incident.

12. We note above a non-exclusive list of examples that would merit disclosure under Item 1.05 of Form 8-K covers some, but not all, types of material cybersecurity incidents. Are there additional examples we should address? Should we include a non-exclusive list of examples in Item 1.05 of Form 8-K?

Example 2 on the non-exclusive list doesn’t specify if the incident is related to a malicious or accidental outage, but example 1 does. Would suggest this is specified as well (do accidental technology outages, unrelated to a malicious actor, which are material in nature also require disclosure?). I presume there will be a period of time, the organization will not know if the incident is accidental or malicious. The full impact will most likely take longer to fully assess.

We support the inclusion of the list of examples in item 1.05

13. Should we include Item 1.05 in the Exchange Act Rules 13a-11 and 15d-11 safe harbors from public and private claims under Exchange Act Section 10(b) and Rule 10b-5 for failure
to timely file a Form 8-K, as proposed?

*It depends on whether the timing is adjusted. If it is not, a safe harbor may be appropriate.*

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?

*It depends on whether the timing is adjusted. If it is not, a safe harbor may be appropriate.*

16. *Should* we require a registrant to provide disclosure on Form 10-Q or Form 10-K when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate, as proposed? Alternatively, should we require a registrant to provide disclosure in Form 8-K, rather than in a periodic report, as proposed, when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate?

Yes. *This situation is common especially when dealing with an Advanced Persistent Threat actor who wants to exfiltrate data and IP over time.*

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?

Absolutely not. *Policies are the board’s statement about its security strategy and risk appetite. They are too valuable to hackers and would probably inflict the organization with all sorts of Monday morning quarterbacking that does nothing to move the ball forward (e.g., needless distractions). On a practical level, an organization of any size would have a huge number of procedures that change fairly often.*

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?

On page 38, Item 2, entitled Governance, we are proposing the language changed to the follow for completeness “…ability to understand how a registrant prepares for, prevents, detects, and responds to cybersecurity incidents…”
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? See supra Section II.B.2, for examples of cybersecurity incidents that may require disclosure pursuant to proposed Item 1.05 of Form 8-K.

This disclosure may be useful. Multiple lines of defense are a fundamental part of any robust cybersecurity strategy. These are essential aspects of existing Governance, Risk Management, and Compliance (GRC) programs. Our goal should be to have Cyber folded into those programs and be a board discussion.

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, that is something a stakeholder would want to know. A registrant should be able to explain why they think they do not need one and why they are not subject to any requirements by all of the jurisdictions they operate in.

The SEC may want to provide for a scenario where a company needs to remain under the radar while they get their cyber hygiene in place.

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?

Yes. The concerns can be grouped into three categories. First, providing hackers too much valuable information. Second, distracting resources during an incident to handle the SEC reporting. Third, disclosing too much about key personnel, including Board Members, makes them a target.

The SEC can handle the first item in much the same way we handle external audits and third party attestations today. We disclose the broad strokes and overall results, not specifics. The second, is to provide the mechanisms mentioned above - heads up during the event with subsequent (more) formal reporting. This would also be subject to input from Law Enforcement, et al (e.g., no public disclosure during an investigation).
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?

*No, if they are required to report to the SEC they should be reporting Cyber like they would any other risk, though with the same exceptions discussed above.*

*The SEC might also want to consider some sort of graduated reporting based on sensitivity of data, and system risk.*

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?

*There should be no requiring names of persons. Instead, require a listing of the qualifications and expertise from the BOD with names being optional so that there are less unintended effects.*

28. When a registrant does not have a person with cybersecurity expertise on its board of directors, should the registrant be required to state expressly that this is the case under proposed Item 407(j)(1)? As proposed, we would not require a registrant to make such an explicit statement.

*It may be helpful for such registrants to report how they fill the gap (e.g., outside SMEs); whether they think it is not necessary or are working towards it in another way.*

31. Would the Item 407(j) disclosure requirements have the unintended effect of undermining a registrant’s cybersecurity defense efforts or otherwise impose undue burdens on registrants? If so, how?

*It could limit the pool of viable candidates. It could also turn board members into targets. Some candidates would also be concerned with extra liability. On balance, the benefits out weigh the risk. There are probably ways around this. Limiting their liability is a good first step and limiting the depth of disclosure would be another.*

35. Should certain categories of registrants, such as smaller reporting companies, emerging growth companies, or FPIs, be excluded from the proposed Item 407(j) disclosure requirement? How would any exclusion affect the ability of investors to assess the
cybersecurity risk of a registrant or compare such risk among registrants?

_Only if driven by the value of the data, value of assets, or system risk not because of their size._

36. Should we adopt the proposed Item 407(j)(2) safe harbor to clarify that a director identified as having expertise in cybersecurity would not have any increased level of liability under the federal securities laws as a result of such identification? Are there alternatives we should consider?

_Yes, they should not have an increased liability in the same way a board member with special expertise in other fields (e.g., accounting)_

Thank you for taking the time to consider our comments.

On behalf of the CSA community,

John Yeoh
Global Vice President of Research, CSA
jyeoh@cloudsecurityalliance.org
2212 Queen Anne Ave N
Seattle, WA 98109
USA