Via *rule-comment@sec.gov*

May 9, 2022

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

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22)

Dear Ms. Countryman:

The Internet Security Alliance (ISA) welcomes the opportunity to comment on the Securities and Exchange Commission's (the SEC's or the Commission's) proposed rules on *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (2022).[i] ISA particularly wishes to thank the Commission staff for meeting with the ISA board to discuss the critical issues raised in the NPRM.

Cybersecurity is not like Enron[ii] or WorldCom[iii] and other high-profile SEC cases where the Commission correctly stands in for the consumer/investor. In the cybersecurity world, the attackers are stealing individual information and value, corporate intellectual property and national secrets. In this space the Commission, industry, the investor, and the government are all on the same side. In addition, we are collectively facing an intensely collaborative attack community. The Commission can best serve the interests of the investor community by helping the rest of government and industry to work collaboratively to build a sustainably secure cyber system. Should the Commission choose to follow some of the comments ISA makes below, ISA would be happy to continue to work collaboratively with the Commission toward that mutual goal.

In 2018, the Commission issued interpretive guidance[iv] to reinforce and expand upon the 2011 guidance. The agency addressed the importance of

cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity. The SEC says that while companies' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since then, disclosure practices are inconsistent.

According to the SEC, its proposed amendments would include these important changes to the agency's reporting requirements:

- Require current reporting about material cybersecurity incidents on Form 8-K.

- Require periodic disclosures regarding, among other things:

    - A registrant's policies and procedures to identify and manage cybersecurity risks.
    - Management's role in implementing cybersecurity policies and procedures.
    - A board of director's cybersecurity expertise, if any, and its oversight of cybersecurity risk.
    - Updates about previously reported material cybersecurity incidents.

EXECUTIVE SUMMARY OF ISA COMMENTS

* ISA has a long history of working to enhance corporate cybersecurity and offers this expertise to the Commission in order to help develop appropriate, useful approaches to disclosures of cyber risk management practices. In ISA's continued effort to enhance corporate cybersecurity, it has developed nearly a dozen open-source products that have been embraced by both industry and government entities (including but not limited to the United States). Included in these products is a set of corporate cyber-risk oversight principles and practices that have been independently assessed and found to enhance a wide range of positive security outcomes. These principles and practices have been described in peer-reviewed academic literature as constituting a "de-facto standard" for appropriate cyber risk oversight and management. They thus can legitimately be considered best practices which the Commission should consider in place of the

undefined strategies, and procedures alluded to in the NPRM Disclosure of these independently assessed and successful cyber risk strategies principles and practices may well be a preferable alternative to the policy and procedures required under the proposed rule as they have been shown to enhance corporate cybersecurity and, hence, demonstrate to investors sound cybersecurity governance, but do not bring any of the potential negative consequences many in industry fear will result if the rule, as proposed, is implemented.

- ISA is concerned that the Securities and Exchange Commission may be underestimating the difficulty of accurately detecting, mitigating and addressing cybersecurity incidents. The commission may also be underestimating the pressures organizations will feel to comply with the new proposed regulations and that hasty judgements, based on short timelines and incomplete data, may well result in inaccurate signals to the market and thus enhance, rather than mitigate, mis-pricing.

* ISA believes it is unclear, based on empirical evidence, if there is need for the new SEC proposed rule on cybersecurity. ISA believes the best course for the Commission to proceed into this area, where it has comparatively limited data and expertise, by following the universally approved process in the cybersecurity field of risk management. A risk management approach would carefully balance benefit and risk based on empirical data. ISA notes that the Commission acknowledges in its NPRM that it currently lacks the empirical data by which to measure the benefits that the NPRM speculates will result from the proposed rule. ISA suggests the SEC commission research leveraging some of the many disclosure systems already in existence to empirically determine the current degree of market mis-pricing under existing guidance and use that as the basis to calculate the amount of benefits the new rules would create. Following the risk management model, these benefits would then be balanced against the risks the new rules will create. ISA suggests that this more deliberate and evidence-based process is especially appropriate in the cybersecurity field, which has direct impacts not only for investors but for broader concerns including national security.

* Form 8-K should specify that any disclosure requirement for a material cybersecurity incident shall only be triggered four days after the company reasonably determines that the incident has been contained (not four days after a

determination of materiality). Many vulnerabilities can be/are embargoed for extended periods once discovered. This is done to give the affected companies time to fix the problem, create patches, or ship the fixes to their customers. Although impact/materiality may be assessed at some point, organizations need time to deal with understanding the scope of the impact and actioning any remediations. Additionally, as will be discussed in greater detail below, information disclosed in "policy and procedure" could provide inference points to an attacker — the unknown or unrealized details about the organization (countries they operate in, JVs, vendors, technologies, domains, *et. al.*) Providing companies with additional time would allow for a more fulsome, accurate, and relevant disclosure to investors. It would be akin to waiting until the firefighters had extinguished all the flames in the building before asking for such key elements as a description of the nature and scope of the fire, an inventory of the property that was damaged, the effect on building operations, and what steps had been taken to prevent future fires. A delayed disclosure obligation would eliminate the risk that the adversary would accelerate or broaden its attack or adjust its tactics upon learning of the disclosure before all vulnerabilities are discovered and patched by the company under attack as well as others that may face similar vulnerabilities. Allowing more time for disclosure also would help cyber first responders focus their valuable time and resources on remediation and recovery from the incident and not devote unnecessary time to crisis communications and public relations while facts are still emerging and being confirmed.

- Any disclosure obligation should apply only to the owner or operator of IT systems, and not the user or customer as currently contemplated by the Proposed Rule. To the extent that a customer is informed of an incident, the customer is often bound by confidentiality obligations and provided limited information. This would make assessing materiality difficult if not impossible.

* ISA is extremely concerned that the disclosures required under the new rule will provide greater assistance to the attack community than to investors and hence, following a risk management theory, the rule, as currently written, should not be implemented. These risks are magnified for certain industry sectors such as Defense Industrial Base (DIB). ISA offers alternative constructions which will allow for adequate investor knowledge of cybersecurity governance and risk

management but not create enhanced cyber risk to investors, industry, and the nation.

* ISA notes that the Commission appropriately raises the issue of regulatory conflict and redundancy with respect to current cyber disclosure rules even noting the inconsistent reporting under current guidance as a reason for the new proposed rules. ISA notes that it is not necessary to expand the rules as done in the NPRM, in order to clarify reporting under current rules and establish greater consistency of reporting. Moreover, ISA believes the proposed SEC rules will significantly exacerbate the problem of regulatory conflict and duplication. Further, ISA emphasizes that the regulatory conflict and redundancy in this space is not simply a case of administrative waste, but seriously impacts corporate, and therefore national, cybersecurity practice as it distracts already very scarce cybersecurity resources, and as such is harmful to investors. ISA suggests the Commission forestall adding to this problem and instead allow the newly created Office of National Cybersecurity Director in the White House to carry out its legislatively mandated process of streamlining the disclosure process, after which point, the Commission can act if necessary.

* ISA believes that the proposed new rules will open the door to potentially substantial stock manipulation triggered by timed negative disclosures which the new rule would facilitate. ISA notes the Commission acknowledges this prospect in the NPRM and argues the proposed 4-day reporting requirement mitigates against this threat. ISA believes the Commission's argument in this case underestimates the ability of the sophisticated attack community (e.g., Cybersecurity attacker group FIN4)[v] to manipulate the new rules. ISA offers alternative actions the Commission can take that would not create this prospect.

WHO IS THE INTERNET SECURITY ALLIANCE (ISA)?

The Internet Security Alliance is a coalition of private sector organizations founded in 2002. The ISA board consists of senior cybersecurity professionals representing virtually every portion of the government identified critical industry sectors.[1] ISA sells no products or services. ISA does not take advertising and does not endorse any products, services, or individuals, including the products and services of its member companies. ISA doesn't have a PAC or a lobbyist. ISA's sole

[1] Internet Security Alliance Board, https://isalliance.org/about-isa/board-of-directors/

mission is to integrate advanced technology with economics and public policy to create a sustainable system of cybersecurity. ISA spends roughly equal amounts of its time focused on public policy as well as corporate cyber risk oversight and management. In addition to numerous other awards, ISA has twice been named to the National Association of Corporate Director's "Corporate 100" list of the most influential organizations in the field of corporate governance.

SEC CAN USE ISA'S EXPERTISE IN PROMOTING EFFECTIVE CYBERSECURITY TO ENHANCE INVESTOR KNOWLEDGE

In 2012, ISA, in conjunction with AIG, approached the National Association of Corporate Directors (NACD) and proposed developing a coherent set of best practices for corporate boards to best implement their responsibility for cyber risk oversight. Over the past decade ISA, in partnership with NACD has produced three editions of the Cyber Risk Oversight Handbook,[vi] which NACD reports is their most popular publication. ISA was pleased to note the Commission cited this work seven times in its NPRM. The handbooks are built around a set of five principles boards should follow to practice good corporate governance of cybersecurity. The handbooks also speak to the required coordination of the board with the management team as they fulfill their role in implementing the cyber risk management function. In summary, these principles are:

- Boards need to address cyber risk at the board level as a strategic enterprise-wide risk and not simply from an "IT" perspective
- Boards need to fully appreciate their unique legal obligations for cyber risk oversight
- Boards need to acquire access to appropriate expertise in cyber risk management
- Boards should require management to develop an enterprise-wide structure to manage cyber risk both from a technological and corporate governance perspective and assure adequate budget and time spent on cyber issues at board meetings
- Boards should require management to perform a comprehensive, empirically based, cyber risk assessment, including the potential costs from cyber events, as well as providing an assessment of which risks they recommend be accepted, rejected, mitigated or transferred and how these

functions will be implemented consistent with the risk appetite and business plan approved by the board of directors.

The handbooks also provide a series of "tool-kits" facilitating boards oversight of the management team on specific cybersecurity issues such as supply chain, insider threat, M&A and economically based cyber risk metrics and others. To our knowledge, the NACD-ISA handbook is the only private sector produced publication that has been endorsed by both the US Department of Homeland Security and the US Department of Justice. ISA is currently working with the NACD on the fourth edition of the US Cyber Risk Oversight handbook, due to be published in 2023.

An article in the March 2021 editions of **Cyber Security: A Peer Reviewed Journal,** "International Principles for Boards of Directors and Cybersecurity," by Larry Clinton)[vii] references to these principles and practices as a "de-facto standard" for appropriate cyber risk oversight and management. Although, in candor, the article was written by ISA President Clinton, the reference appears in a peer-reviewed professional journal. That taken with the multiple endorsements from both industry and government around the world would seem to appropriately qualify these principles and as best practices which the Commission should consider in place of the undefined and unassessed strategies, and procedures alluded to in the NPRM.

In addition, since the NACD-ISA principles are clearly articulated and consistent across multiple domains they would provide a clearer guide for industry, the investor community and the Commission in assessing if an organization is appropriately engaging in cyber risk management and oversite. As such these practices are preferable in many respects to the rule in the NPRM.

ISA has also developed adapted versions of this handbook for use around the world. There are now 10 separate editions of the handbook available on four continents and in five languages. These include a German edition in partnership with Germany's Federal Information Security Division – BSI – and the Cybersecurity Foundation of Germany (a second edition has been completed and will be release later in 2022), a pan-European edition developed in partnership with the European Council of Directors Associations, a Latin American edition developed in cooperation with the OAS, a Japanese edition developed in

cooperation with the Japanese Business Federation, an Indian edition developed in partnership with the Associations of Indian Infrastructure Organizations, and an East-Asian edition in partnership with AIG. This year ISA also produced a separate edition targeted at college/university and foundations in conjunction with the Association of Governing Boards.

These Cyber Risk Handbooks are one of the only sets of best practices to have been *independently assessed and found to generate tangible pro-security outcomes.* PWC, in their annual Global Information Security Survey reported that organizations that used the principles highlighted in the handbook experienced a range of positive security outcomes including better cyber risk management, closer alignment between cybersecurity and overall business goals, better cyber budgeting, and creating a culture of security. In 2021 the World Economic Forum joined ISA and NACD in promoting a similar set of cyber best practices for corporate boards adding a sixth principle which called upon corporate boards to extend their oversight of cyber risk to their full eco-system, not just that of their own organization. This sixth principle will be added to the 2023 US edition of the NACD-ISA Cyber-Risk Oversight handbook.

The Commission's NPRM speaks not only to the need for boards to engage in effective cyber risk oversight activity, but management as well. ISA agrees with the need for a coordinated and coherent board management partnership. To that end, ISA has published a new book that takes the cyber risk oversight principles and toolkits detailed in the handbooks and translates them down to the management level. This book, Cybersecurity for Business: Organization-Wide Strategies to Ensure that Cyber Risk is Not (just) an "IT" Issue has been #1 on Amazon's Hot New Releases list for the past month and has already been accepted for use in cybersecurity courses at Columbia, Wharton, NYU, and Indiana University.

As will be discussed in more detail below, it is not the concept of disclosure about cybersecurity that is problematic as much as the types and methods of disclosure that ISA urges be reconsidered. ISA believes that requiring public companies to disclose if they follow a set of independently assessed cyber risk oversight and management principles, such as those articulated in the NACD-ISA handbooks, will provide investors with a much clearer understanding of how cyber risk is being addressed by an organization, without carrying with it the risk

of weakening the security enterprise, enhancing stock manipulation or wasting scarce cybersecurity resources.

THE COMMISSION MAY BE UNDERESTIMATING THE DIFFICULTY IN PROPERLY ASSESSING AND MANAGING CYBER ATTACKS

While filing a series of reports to the Commission may not be difficult, especially for a larger organization with a sophisticated compliance infrastructure, accurately detecting, analyzing, mitigating, and assessing cyber attacks is extremely complicated.

ISA believes it is worth noting on the outset that cybersecurity is fundamentally different than many traditional Commission areas of inquiry. Most cyber incidents of significance are more the result of the unbalanced economics of the digital age than corporate misfeasance or malfeasance.

In the cybersecurity field virtually all the economic incentives favor the attacker. Cyber attack methods are comparatively cheap and easy to acquire, the profits from successful attacks can me be massive the attackers' business model is very favorable (they can use the same methods all over the world repeatedly). The defender community very often is completely out-resourced by the attacker, while defending an immense and inherently vulnerable system (the internet was built to be an open system) and there is almost no law enforcement. We successfully prosecute less than 1% of cyber criminals.

Cyber attacks are often engineered by sophisticated, well-funded (often better-funded than the victims) actors who may be nation states or state affiliated. Even many of the criminals not directly associated with governments, have been trained by those governments, have tools equivalent to that of the nation state and are allowed to carry out these activities with impunity to prosecution. ISA fears the Commission may be underestimating the difficulty involved in determining accurately the impact of the crime or even the extent of the crime scene especially while in the process of mitigating it.

To take a well-known example, consider the case of the SolarWinds incident. FireEye publicly disclosed a breach into their environment on Dec 8,

2020. They cited “we are actively investigating in coordination with the FBI and other key partners, including Microsoft”, suggesting the investigation had been ongoing for some time and potentially back to November. Although numerous portions of the federal government had been successfully compromised by the attack, the broader government was unaware until notified — voluntarily — by the private sector. Based on knowledge at the point of detection it was apparent that this was a severe attack — quite possibly material — but the extent and how to respond took weeks to plan. On December 13, 5 days later, FireEye provided a follow-up blog post and customer call identifying SolarWinds as the source of the initial intrusion. FireEye filed an 8-k on December 13 and SolarWinds on December 14. Per the proposed timelines, 8-K disclosure would have been required while the parties were still investigating, coordinating response actions, preparing to notify customers, working with authorities, etc. FireEye’s response to the SolarWinds incident is viewed in the cybersecurity field as “what good looks like.” The SEC proposed requirements would suggest it was not fast enough.

The SEC’s proposal to require reporting of material cyber incidents to investors within four business days of determining the incident is material will create situations in which companies would be required to make complex determinations on materiality with a dearth of information available at early stages In clarifying its expectations under the new proposed rule the Commission states The Commission notes that if it adopts the date of the materiality determination as the Form 8-K reporting trigger, the agency would expect registrants to be “diligent in making a materiality determination in as prompt a manner as feasible.” The agency adds that “‘a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident’” to address the belief that some companies may delay making such a determination to avoid a disclosure obligation.

As such, the new rule will very likely create inordinate pressure for hasty reporting which will lead to the very mis-pricing the Commission is trying to prevent as well as far greater risk such as to national security. CISO’s on the ISA board have reported that many times they have led investigations into incidents that looked really bad that turned out to be much less damaging once the full picture became apparent.

In still a different scenario the judgement on likely materiality may be quickly apparent, such as in a ransomware attack where the demand is clearly a material hit to the company. This virtually instantaneous reasonable judgment of materiality could precede accurate analysis and mitigation, which could take weeks or months depending on the unique situation. Yet, under the proposed rule, the victimized company may reasonably be in no position to make an adequate and useful report after 4 days, even with 100% whole-hearted efforts.

The FireEye/SolarWinds example deals with highly sophisticated companies. As another example consider a mid-sized company that discovers an incident/intrusion but is unsure of the extent of impact. There will be substantial internal pressure from Risk & Compliance to meet the new SEC reporting timelines. If discovered on a Monday, and if it has the potential to be material, the risk department will very likely push teams to report on Friday. The experience of ISA board members suggests that for a company that will need outside help, the timeline is unrealistic, and could very well mis-inform investors.

Given the immense complexity of the technologies, the business methods, the attack vectors, and the uniqueness of many of the most serious cyber attacks the ISA recommends that the Commission return to its previous view that guidance, as opposed to strict regulation is the most appropriate position for the SEC to take with respect to cybersecurity. While ISA appreciates the Commission's desire for consistency in reporting, the reality is that the traditional "one-size-fits-all" regulatory model is inappropriate to dealing with the highly dynamic and idiosyncratic space of cybersecurity. Clear guidance is a better model.

In addition, the proposed SEC rule defines a cybersecurity incident to include an unauthorized occurrence on or through a registrant's "information systems," the proposed definition of which would include information resources "***owned or used"*** by the registrant. We believe this language is problematic because a company may ***use*** many systems to process its data, including vendor systems used in numerous software-as-a-service, platform-as-a-service, or infrastructure-as-a- service offerings provide by external vendors, over which it has no operational control. In such circumstances, where companies often rely on such vendors to inform them of details of cyber incidents impacting the vendor systems, companies may have particular challenges in obtaining sufficient

information from the vendors (who in turn may be hesitant to promptly share detailed incident information with the company due to liability concerns) to make an informed materiality determination.

ISA also suggests that the amount of disclosure from multiple separate entities involved in corporate supply chains required by the proposed rule could create an avalanche of reports from widely varied perspectives based on organizations inter-relationships. This cacophony of reports may be extremely difficult for investors (and possibly the Commission) to navigate and clearly comprehend, which will not only undermine the benefit the Commission hopes for but enhance mis-pricing.

ISA recommends that at minimum, in the definition of "information systems,", change "owned or used by the registrant" to "owned or operated by the registrant," since companies can more reasonably be expected to timely obtain sufficient information about incidents on systems that they own or actually operate.

ARE THE COMMISSION'S NEW PROPOSED RULES NEEDED?

Unlike traditional financial compliance wherein an organization can be determined to be in compliance or not (pass-fail) cybersecurity is different. Cybersecurity is best understood as a range – one is not secure vs. insecure. Leaders in cybersecurity engage in a systematic and empirically based risk assessment process that balances risk vs benefit. Simply reviewing a checklist of policies and procedures will tell an investor little about the actual cyber risk posture of an organization. What is more informative is the methods the organization uses to assess its unique cyber risk, determine its unique cyber-risk appetite, and allocate resources. Descriptions of the actual strategies, practices and procedures is unnecessary and likely not truly informative and can even create misinformation.

The SEC's proposal to require reporting of material cyber incidents to investors within four business days of determining the incident is material will create situations in which companies would be required to make complex determinations on materiality with a dearth of information available at early stages of the incident, while also potentially making disclosures with incorrect

information. Sophisticated cyber events are often characterized by ingenious methods designed to create mis-direction. Hence, "timeliness" must not be confused with haste.

A 2022 IBM study reported that, in 2021, it took an average of 212 days to identify a breach and an average 75 days to contain a breach, for a total lifecycle of 287 days. It is now cliché to note that much is unknown in the early hazy days of an incident, including the type and scope of information potentially impacted. It is likely that such a short disclosure timeframe would lead to rushed disclosures of information that ultimately turns out to be incorrect, thus creating a disservice to investors and at least a temporarily impact to the pricing of securities, based on such incorrect information. Thus, the proposed rule may create the very mis-priced value – the Commission is hoping to address.

Moreover, recent independent research indicates that actual material cyber incidents are quite rare Given the inherent vulnerability of digital systems (the Internet itself was built as an open system) cyber risk policies are best considered on a risk management basis which carefully weighs cyber risk vs. costs. Any benefits of cyber disclosure need to similarly be carefully balanced with other considerations including organizational and national security.

In its NPRM the Commission asserts that the value of "timely disclosure" to shareholders outweighs the risks of premature disclosure but provides very little evidence to support this assertion. In fact, the NPRM states: "we are unable to quantify the potential benefit to investors and others as the result of increased disclosure and improvement in pricing under the proposed amendments. This estimation requires information about fundamental value and extent of mispricing. We do not have access to such information."

It's important to note that the Commission already has strong guidance in place for appropriately disclosing cyber events that would materially impact investors. Independent research suggests these rules are adequate and effective. For example, a 2022 study of 1,200 large companies by ThoughtLab found the percentage of breaches that were "material" (defined as "generating a large loss, compromising many records, or having a significant impact on business operations") was less than 1% of all breaches – .07 % in 2021 and .08% in 2022**.** The Commission's NPRM itself cites a study indicating that firms with higher cyber

risk have a higher cost of capital which suggests investors operating under current guidance are aware of and considering cyber risk.

In its NPRM, the Commission does not contend that cyber *incidents* impact investors, only that *disclosure of cyber incidents"* impacts shareholders. However, the vast majority of cyber attacks are not publicly disclosed, and probably ought not be because, current research suggests the vast majority of such incidents are not material. Since it is the *disclosure* of events that impacts stock prices and the new rule will increase disclosures, the new rule runs the risk of taking immaterial events and turning them into material events via disclosure – all without clear evidence of how much the disclosures will help the investors.

Given that the extent of current disclosure about cyber events under the SEC guidance is well above 1%, it would seem the current guidance is working effectively. A more tailored study testing the Commission's theory that cyber incidents create mispricing or market asymmetry might be prudent.

ISA recommends that before proceeding into this area of undocumented benefit and potentially high risk, the SEC commission research leveraging any of the many existing cyber disclosure models and determine if their hypothesis of the fundamental value or mispricing exists and to what extent. Based on this empirical risk management approach the Commission will develop more grounded and effective public policy and thus protect investors appropriately.

THE COMMISSION'S NEW PROPOSED RULE WILL LIKELY ASSIST ATTACKERS MORE THAN INVESTORS

The NPRM acknowledges that there is risk that their more extensive disclosure may increase the risk of attack but suggests this added risk might be mitigated due to increased security efforts responsive to the new rule. In the end the academic literature on this issue is inconclusive.

Obviously, there is substantial debate as to exactly what information will be, should be, or must be disclosed under the new proposed rule, and when. However, we do know that the attack community is highly sophisticated – often nation state affiliated. Accordingly, whatever information is disclosed under the

proposed rule will more likely be better understood and of more use to the expert attacker community than it will be for the typical investor.

The disclosures will either be informative or not. If disclosures of security policies and procedures are sufficiently informative for an investor to make a reasoned judgement about the security of an entity, it will almost, by definition, be informative enough to provide useful information to attackers. Conversely, if the information is not useful to the attack community with all its expertise and cybersecurity specific resources, it is difficult to believe it will be sufficiently informative to the investor to make a well-informed judgment on the company's security.

Even if the Commission could somehow craft a "Goldilocks" solution – just the right information for the investor, but not enough to aid the attacker – maintaining that balance in the highly volatile cybersecurity environment will be virtually impossible.

ISA notes, because it may take companies longer than four business days to contain a major cyber incident, requiring public disclosures about an incident before it is internally contained could tip off bad actors to the fact that a company is presently vulnerable to cyber attacks, leading to additional cyber attacks. During that remediation period, there is a significant concern that any disclosure of the matter could cause other attackers to "piggyback" and attack the company. It has been argued by some that the opposite would occur, i.e., that "*hackers would stay away from a company handling a breach as it would be a harder target now, as the company would be considered to be better prepared to defend itself.*" ISA finds that argument to be wishful thinking. In several instances, including the recent example of T-Mobile[viii] , a company that has been attacked and disclosed 6 breaches in the past four years, we have seen attackers repeatedly going after a previously compromised target.

Attackers are often sophisticated enough to know that virtually all organizations suffer from a shortage of cybersecurity resources. These resources will only become more stressed while addressing a sophisticated attack (which may still be on-going) and will be additionally diverted by simultaneously compiling with SEC (and likely other) regulatory compliance procedures. Attackers are aware of this and will almost certainly "smell blood in the water" and pile on

additional attacks against the weakened and distracted target. Moreover, attackers have an almost unlimited amount of attack methods, so the fact that an organization is fending off attack method "A" does not necessarily assist them when they then need to address attack method "B" (and possibly C, D, E, F, & G) from multiple attackers.

Finally, under the new proposed rules, the company may be required to publicly report the existence of a zero-day vulnerability in vendor software used by many other companies. This disclosure would appear to be required without a chance to responsibly report the vulnerability to the software vendor in confidence and allowing them a chance to issue a patch before the vulnerability is publicized. Public disclosure of such unpatched, zero-day vulnerabilities could tip off bad actors to look for other victims using the software (e.g., the SolarWinds case) to attack, leading to additional cyber attacks across industries. Additionally, it is also costly and impracticable for issuers to continuously monitor third party systems. It is unfair to hold a company liable for disclosures related to events that it does not control. At a minimum, the SEC should give companies a safe harbor against liability for failure to disclose a third-party breach.

ISA suggests the Commission alter its focus for disclosure away from security policies and procedures and toward information that will be more helpful for the investor and less helpful to the attacker.

One example would be reporting the costs of cyber events to the organization. ISA suggested that a disclosure of the actual "costs of cyber" within the organization may be more informative to investors than a disclosure of cyber practices and policies which investors may reasonably not understand. With cost information, investors can make their own determinations of the significance cyber attacks have on the company and can track if these costs are being increased or reduced . The costs would be a clear, objective measure that could also be compared to that of industry peers. While cost data on cyber incidents would provide the investor with a practical insight as to the ability of an organization to manage its cyber systems it would not provide any useful data to malicious actors that might enable future attacks.

Alternatively, a disclosure of what models the organization uses to make its cyber risk assessment, without disclosure of specific policies and procedures

that result from that assessment, could be disclosed These sophisticated models (e.g., X-Analytics, FAIR, or Security Q) are publicly available and, thus, investors could use them to gauge the sophistication of the organization is assessing and managing risk without disclosing specific practices and procedures which will be useful to the attack community.

At minimum, ISA urges the SEC to reevaluate the trigger for reporting within four business days of determining that it has experienced a material incident and allow for reporting to occur after the company has had a reasonable opportunity to respond to and resolve the incident. We also urge the SEC to specify that companies do not have an obligation to describe with particularity in their reporting the details of any vulnerabilities in their systems that they reasonably believe could assist cyber attackers, or details of vulnerabilities in third-party software that have not been disclosed by the third-party software vendor.

ANY NEW RULE NEEDS TO INCLUDE EXCEPTIONS FOR NATIONAL SECURITY AND LAW ENFORCEMENT

The lack of an exception to allow delay of reporting of material incidents in cases where disclosure could negatively impact national security equities, or a law enforcement investigation could be detrimental to national security and law enforcement investigations against cyber attackers. Relatedly, we are concerned that in the rush to comply with a 4-business-day reporting deadline, companies that have experienced cyber incidents impacting classified information may be put in an impossible situation of choosing between violating SEC disclosure obligation and violating criminal statutes, prohibiting unauthorized disclosure of classified information, given lack of time to properly vet and redact classified information from the disclosure in coordination with the government.
ISA suggests the Commission include a provision to allow delay of reporting of material incidents when the company has been informed by government authorities that a delay in disclosure would be in the interest of national security or an ongoing law enforcement investigation, and specifically clarify that companies do not have an obligation to describe with particularity in their reporting any information related to classified information, system, or programs.

ANY NEW RULES NEED TO BE UNAMBIGUOUS TO ASSURE THE CONSISTENCY THE COMMISSION DESIRES

The Commission correctly identifies regulatory inconsistency as a major problem; however, this inconsistency will likely be exacerbated under the proposed rule. Specifically, the SEC's proposal to require companies to disclose when a series of previously undisclosed, individually immaterial, cybersecurity incidents has become material in the aggregate, creates an exceptionally ambiguous standard. We believe this to be a highly subjective and potentially imprecise calculation that is practically unworkable. ISA suggests the Commission remove this proposed requirement.

THE NEW SEC PROPOSED RULE WILL EXACERBATE THE CRITICAL SHORTAGE OF CYBERSECURITY RESOUCES

ISA is concerned that the SEC action will be adding another federal layer of federal regulation on top of what already exists, further complicating the already confused process of managing cyber risk.

A GAO study last year documented that that complying with redundant and conflicting federal cyber regulations costs states and localities up to 70% of their meager cybersecurity budgets. This government study replicates the findings of previous research, which has found similar problems with duplicative and redundant regulation on the private sector.

A 2022 study by ThoughtLabs found that 28% of the CISO's it surveyed reported that the increasing complexity of the varying cyber regulations itself is now among their greatest cyber risks, as it pulls scarce cyber resources into regulatory compliance activities when the organization needs them to be focused on security.

Requiring multiple, largely duplicative reports detracts from managing cyber risk. One fact virtually everyone in the cybersecurity space agrees on, both government and industry, is that we don't have nearly enough cybersecurity practitioners. The Bureau of Labor estimates that the current gap between cybersecurity jobs and qualified people is over 300,000 (some report this as closer to 600,000) and growing fast as attacks are rapidly mounting. As a result, it is

imperative that we use our scarce cybersecurity assets as efficiently and effectively as possible to mitigate risk.

The NPRM itself notes that greater uniformity would be a positive step, however, the SEC doesn't need to expand its requirements in order to streamline them. Moreover, such uniformity is fleeting if it only applies to the SEC disclosures.

The NPRM acknowledges that at least in some cases the Commission's new rules would conflict with some state cyber disclosure laws which grant exceptions to allow law enforcement to carry out criminal investigations. The Commission acknowledges this conflict but asserts that it is justified because the purpose of the two disclosures differs (investor information vs. law enforcement investigation).

Although the Commission is correct that the purposes of the two provisions are distinct, that makes little difference to the entity that will still need to waste scarce cyber resources, to engage in the dual processes, to provide basically the same disclosure.

Moreover, it is highly questionable that it is more important, on balance, to give a distinct set of investors "timely" information about one company than it is to aid law enforcement and, thus, protect all investors by potentially prosecuting cyber criminals and, thus, preventing many further attacks.

A sustainably secure cyber environment can only be accomplished by industry and government working in partnership. The additional tension that can be created through layering another administrative regulation, with the enforcement that will likely follow, is not in the spirit of needed cooperation.

It is notable that as the federal government's cybersecurity practices have matured, they have increasingly begun to move away from seeing industry as just a "stake-holder" and view it more as a real partner. Government is probably more dependent on industry in this fight than the other way around and a great deal of effort has gone into creating an increasingly collaborative model.

Finally, ISA notes that the recently created Office of National Cybersecurity Director (ONCD) in the White House has been charged to coordinate, deconflict, and harmonize" federal incident reporting requirements, including those issued through regulations. ISA suggests the SEC communicate to the ONCD requesting they accelerate their streamlining process. The SEC should forestall implementing any new requirements in this area until the ONCD has completed its streamlining process allowing for a cohesive and efficient national policy on cyber incident reporting.

THE SEC'S NEW PROPOSSED RULE COULD INCREASE STOCK MANIPULATION

There is also the very real possibility that the new rules would open the door to stock manipulation. The NPRM itself suggests the possibility of malicious actors, such as FIN4, may trade ahead of an incident disclosure to manipulate the market. The Commission argues the new rules will mitigate this risk by mandating that a disclosure be made no more than four days after a breach is judged by the company to be material.

However, that analysis fails to appreciate the degree of control the attackers can have not only on when the attack occurs, but when it will be discovered and likely deemed material. Sophisticated breaches are very well concealed and often are not discovered for months after penetration. The Solar Winds breach was not discovered for at least nine months after the attack – and even then, the federal government had to be told it had been compromised (in nine different agencies) by a private company. Since the attacker has substantial control over the attacks and can often make the attack apparent at a time of their choosing thus starting the clock on the disclosure, they are not truly governed by the 4-day rule.

Because cyber attackers are not governed by the rules of materiality, in most instances the attacker will have ample time before it is discovered and, during this time, it can carry on whatever manipulation, such as shorting stocks, it chooses. Sophisticated attackers will be able to time the disclosure by manipulating the attack to make it known to the victim when they desire. They will then have high confidence of the timing of the discovery and disclosure. If anything, the new rules would seem to provide an incentive for criminals to deliberately stage an attack on a company, after shorting the stock, thereby

triggering the disclosure so as to reap a benefit from the short. In fact, this new rule probably enables the attackers to carry out this scheme with far greater precision potentially shorting multiple companies. As such the Commission's new rule might actually enhance the opportunities for stock manipulation
Unless fuller assurances can be provided that the new proposed rule will not enhance stock manipulation this risk alone strikes ISA as reason to forestall the rule in place and contemplate the other methods of disclosure we have suggested.

---

[i] Securities and Exchange Commission. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 FR 16590, (March 23, 2022). File Number S7-09-22.

https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

Securities and Exchange Commission. SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, March 9, 2022.

https://www.sec.gov/news/press-release/2022-39 (press release)

https://www.sec.gov/files/33-11038-fact-sheet.pdf (fact sheet)

[ii] Weil, J. and Wilke, J. (2002). "Systemic Failure by SEC Is Seen in Enron Debacle," *The Wall Street Journal,* October 7, 2002. https://www.wsj.com/articles/SB1033944629262271233?msclkid=43db2923cfae11ec8ffdcea128f0fe29; "Spotlight on: Enron," United States Securities and Exchange Commission, https://www.sec.gov/spotlight/enron.htm?msclkid=43da6db6cfae11ecacbaf063130968e2

[iii] Securities and Exchange Commission v. WorldCom, Inc, Civil Action 02 CV 4963 (S.D.N.Y.) (June 27, 2002). https://www.sec.gov/litigation/litreleases/lr17588.htm#:~:text=Securities%20and%20Exchange%20Commission%20v.%20WorldCom%2C%20Inc.%2C%20Civil,Affiliates%2C%20and%20the%20Appointment%20of%20a%20Corporate%20Monitor?msclkid=b00133b6cfb211ec80ee0ff679092277

[iv] Securities and Exchange Commission. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, February 21, 2018. https://www.sec.gov/rules/interp/2018/33-10459.pdf

In 2011, the SEC's Division of Corporation Finance issued interpretive guidance to provide the Division staff's views concerning a registrant's (or a company's) existing disclosure obligations relating to cybersecurity risks and incidents.

Securities and Exchange Commission. CF Disclosure Guidance: Topic No. 2, Division of Corporation Finance, October 13, 2011. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[v] Vengerik, B,, Dennesen, K,, Berry, J., & Wrolstad, J. "Hacking the street? FIN4 likely playing the market," *Mandiant,* September 2021. https://www.mandiant.com/resources/hacking-the-street-fin4-likely-playing-the-market

[vi] NACD and ISA. Cyber-Risk oversight 2020: Key Principals and Practical Guidance for Corporate Boards, NACD, 2020, https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298

[vii] Clinton, Larry (2021, March 1). International principles for boards of directors and cyber security. In the *Cyber Security: A Peer-Reviewed Journal*, Volume 4, Issue 3.

[viii] Page, C. Lapsus$ hackers targeted T-Mobile source code in latest data breach," *TechCrunch*, April 22, 2022. https://techcrunch.com/2022/04/22/lapsus-hackers-t-mobile/#:~:text=T%2DMobile%20has%20confirmed%20six,previous%20data%20breaches%20since%202018.