Via Electronic Mail

July 2, 2025

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Re: Petition for Rulemaking on the SEC Rule titled Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.[1] **Petition to reinstate proposed Item 407(J) of Regulation S-K requiring director cybersecurity expertise disclosure from the Proposing Release.**

Dear Ms. Countryman,

We are petitioning the Securities and Exchange Commission pursuant to 17 CFR §201.192 of the SEC's Rule of Practice, to amend the SEC's Cybersecurity Risk Management Strategy, Governance and Incident Disclosure Rule to reinstate the originally Proposing Release rule that recommended amending Item 407(j) of Regulation S-K requiring director cybersecurity expertise disclosure.[2]

This petition is submitted by Digital Directors Network[3] and on behalf of Tenable Holdings, Inc.[4], Allegis Cyber Capital[5], X-Analytics,[6] Cyber Future Foundation,[7] National Technology Security Coalition,[8] HiddenLayer,[9] Pan Asian American Business Council,[10] AI Guardian,[11] and the Information Systems Security Association (ISSA)[12] to reinstate the director cybersecurity expertise disclosure requirement included in the Proposing Release to address the material boardroom cybersecurity leadership control gap and weakness that is growing in the American business system.

EXECUTIVE SUMMARY

Strengthening the boardroom as a leadership control in the cybersecurity systems that protect the value created by American businesses serves investor interests and builds cybersecurity resiliency in the American economy. Director cybersecurity expertise is a common-sense, inexpensive, irreplaceable, and high ROI control in cybersecurity that is proven to work to make the entire cybersecurity system stronger.

Investors deserve an active and effective boardroom capable of governing this material business risk. Evidence demonstrates that boardroom cybersecurity effectiveness is strengthened, and cybersecurity risk is reduced with director cybersecurity expertise on the board.

There is no mitigating control for the lack of director cybersecurity expertise in the boardroom. The absence of this material cybersecurity leadership control creates a critical weakness, which evidence shows causes the boardroom to play a largely symbolic and ineffective role within the cybersecurity system, making cybersecurity less effective than it otherwise should be.

We commend the SEC on the Final Rules related to Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure as long overdue, common-sense, useful, and material information for investors that is also helpful to issuers in advancing key processes in cybersecurity risk management and governance. These are easily implementable rules that better inform investors about cybersecurity risk and its impacts, which are also forcing companies to critically think and mature their processes in cybersecurity risk management.

However, the critical boardroom cybersecurity leadership control weakness that is manifested by the lack of director cybersecurity expertise in the boardroom will always impair the potential to optimize effective and resilient cybersecurity systems in America's companies.

As such, we are requesting that the original proposed director cybersecurity expertise disclosure provision be reinstated, as was previously drafted, in its entirety.

THE PROPOSED RULE

The previously proposed rule stated the following:

> We propose to amend Item 407 of Regulation S-K by adding paragraph (j) to require disclosure about the cybersecurity expertise of members of the board of directors of the registrant, if any. If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s) and provide such detail as necessary to fully describe the nature of the expertise.
>
> The proposed requirements would build upon the existing disclosure requirements in Item 401(e) of Regulation S-K (business experience of directors) and Item 407(h) of Regulation S-K (board risk oversight). The proposed Item 407(j) disclosure would be required in a registrant's proxy or

information statement when action is to be taken with respect to the election of directors, and in its Form 10-K.

Proposed Item 407(j) would not define what constitutes "cybersecurity expertise," given that such expertise may cover different experiences, skills, and tasks. Proposed Item 407(j)(1)(ii) does, however, include the following non-exclusive list of criteria that a registrant should consider in reaching a determination on whether a director has expertise in cybersecurity:

- Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner.
- Whether the director has obtained a certification or degree in cybersecurity; and
- Whether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.

Proposed Item 407(j)(2) would state that a person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including, without limitation, for purposes of Section 11 of the Securities Act (15 U.S.C. 77k), as a result of being designated or identified as a director with expertise in cybersecurity pursuant to proposed Item 407(j). This proposed safe harbor is intended to clarify that Item 407(j) would not impose on such person any duties, obligations, or liability that are greater than the duties, obligations, and liability imposed on such person as a member of the board of directors in the absence of such designation or identification. This provision should alleviate such concerns for cybersecurity experts considering board service. Conversely, we do not intend for the identification of a cybersecurity expert on the board to decrease the duties and obligations or liability of other board members.[13]

The Proposed Rule is a simple disclosure rule, as such it is not cumbersome or overly directive, which makes it easily implementable while giving issuers sufficient latitude and total control over the decision to add director cybersecurity expertise to the board while also considering other director capabilities and needs unique to their particular requirements, e.g., sector expertise,

Those who believe that they do not need director cybersecurity expertise in the boardroom can purposefully act according to their needs and convictions. However, the presence of director cybersecurity expertise on the board, or lack thereof, and a board's deliberate choice regarding this fundamental cybersecurity control is material investor information in either circumstance that could alter an investor's risk assessment of the issuer, given the material business risks presented by cybersecurity.

The Proposed Rule suggests a broad enough definition of "cybersecurity expertise" that encompasses applied knowledge in cybersecurity gained through experience in cybersecurity, along with the formal and structured acquisition and verification of cybersecurity knowledge. This allows issuers to have a sufficiently large pool of highly qualified potential director candidates to choose from while also giving them flexibility in selecting a director cybersecurity expert most appropriate to their specific needs.

The Proposed Rule does not mandate the addition of director cybersecurity expertise, leaving the decision entirely up to issuers. Although it was widely expected that most issuers would respond by adding director cybersecurity expertise to the boardroom, as was pointed out in the public commentary to the Proposing Release.

We believe that this would have happened as well and celebrate it as the needed outcome. This reaction to the simple accountability that disclosure brings, in and of itself, suggests the tacit recognition of the need and value of director cybersecurity expertise in the boardroom.

Precedent exists for this outcome as this occurred with a similar boardroom disclosure provision for qualified financial expertise created by the Sarbanes-Oxley Act of 2002, which brought director financial expertise into the boardroom, for all issuers, for the first time. The universal corporate governance control of director financial expertise strengthened the financial reporting system for each company within the U.S. capital markets, bringing systemic integrity and trust to the entire market system.

This is precisely the systemic outcome needed in cybersecurity governance. The presence of this critical cybersecurity leadership control in each boardroom will build a systemically strong and resilient cybersecurity environment for the entire American business ecosystem.

RATIONALE FOR THIS PETITION

Our reason for submitting this petition is motivated by a desire to solve the root cause of the chronic and growing cybersecurity weakness in American business — **the material cybersecurity leadership control gap and weakness that exists in the corporate boardroom, which is created by the absence of director cybersecurity expertise on most corporate boards.**

When a material leadership control is weak in cybersecurity, the entire cybersecurity system suffers and is weaker than it should be. Recent research indicates only 12% of the S&P 500 can claim true levels of director cybersecurity expertise on the board, i.e., applied experience and knowledge of cybersecurity risk management policies and practices.[14]

Closing this persistent boardroom cybersecurity leadership control gap and weakness will strengthen the boardroom as a key control in the cybersecurity system, making the entire cybersecurity system stronger and more resilient. Without a strong cybersecurity leadership control in the boardroom, America's cybersecurity systems will remain perpetually underperforming.

Two issues have converged since the Final Rules that support our petition to reinstate this simple and highly effective cybersecurity leadership control.

First, evidence continues to grow and demonstrate that director cybersecurity expertise in the boardroom reduces cybersecurity risk. Moreover, without director cybersecurity expertise on the board, corporate governance over cybersecurity risk is shown to be largely symbolic, which does not serve or fulfill the fundamental purpose of the board or serve investor interests. Investors deserve to know if this basic boardroom cybersecurity leadership control is in place due to the material business risks that face their investments from cybersecurity risk.

Second, the cybersecurity risk landscape is continuing to expand, shift, and become increasingly complex. This demands that corporate governance adapt to become an effective cybersecurity leadership control. Boardroom leadership, effectiveness, and adaptability in cybersecurity can only be achieved through the presence of director-level cybersecurity expertise in the boardroom.

Moreover, certain controls are so foundational that they require government regulation to establish a universal standard that strengthens shared interests and risks. Having a director with cybersecurity expertise in the boardroom is such a control.

In a world of distributed but co-dependent cybersecurity risk, one company's control failure can create risk for thousands of other companies. Systemic cyber risk continues to compound and expand with today's complex digital systems and is also becoming more complex and impactful with artificial intelligence (AI) systems. Systemic cyber risks have manifested themselves in high-profile cybersecurity incidents that originated at SolarWinds and CrowdStrike, amongst others, and adversaries are increasingly targeting systemic weaknesses.

Regulation that addresses the boardroom cybersecurity leadership control for each company through reinstatement of the director cybersecurity disclosure rule will quickly and efficiently lead to a collective strengthening of the entire American cybersecurity system. This will create collective resilience and strength throughout the American economy that is more capable of effectively protecting investor interests from the fast-moving, compounding, and catastrophic cybersecurity threats that can rapidly move between companies and materially impair economic growth and output.

With the advancement of AI, systemic risks will also continue to propagate, but the collective ability to mitigate these risks will not advance unless the boardroom is strengthened as a leadership control in America's cybersecurity systems. Boardroom cybersecurity leadership and effectiveness materially and positively impacts the development of a strong and resilient cybersecurity system throughout America's economy.

Effective boardroom cybersecurity leadership and the systemic strength delivered through the presence of director cybersecurity expertise in each corporate boardroom is one of the most impactful and easily implemented controls that will reduce the cybersecurity risk profile of the American business ecosystem.

DIRECTOR CYBERSECURITY EXPERTISE IS PROVEN TO REDUCE CYBERSECURITY RISK

A growing body of evidence demonstrates that when there is a director with cybersecurity expertise on the board, a more effective and resilient cybersecurity system exists within the company.

The growing base of applied evidence from the early adopters and leaders who are adding directors to the board with cybersecurity expertise illustrates some of these specific issues. Evidence from those who have experienced these benefits first-hand includes:

> …the overall consensus was that [cybersecurity] expertise enables directors to provide proactive, value-added oversight of cybersecurity risk that wouldn't be possible without it.

> [L]ack of expertise leads to superficial, check-the-box oversight. For example, board members may simply not give adequate attention to cybersecurity, since directors naturally focus on things they know best. They may ask the CISO naive or off-the-shelf questions that don't cut to the heart of the company's cybersecurity risks.
>
> When answers are provided, [non-expert] directors may not understand them, or be able to detect rosy framing or ask follow-up questions to probe if the CISO or their program needs a shift in direction.
>
> The benefits of directors with cybersecurity expertise include that they "can talk with the CISO" to fully understand issues and challenge the CISO's cybersecurity programs when needed. They can also be a tremendous asset to the CISO by acting as a go-between with the board and by lending political capital to the CISO's requests to the C-suite for resources and needed organizational changes.[15]

These observations and experiences were augmented by additional research from the same Virginia Tech Professors with in-depth field research during 2024, adding more evidence that demonstrates the benefits of director cybersecurity expertise as a cybersecurity leadership control. Their research found that:

> Although nonexpert [cybersecurity] directors may genuinely seek to provide diligent oversight, without expertise, their efforts lack substance and therefore are mostly symbolic, even when they perform the same oversight activities as expert directors.
>
> ...we find that a lack of cybersecurity expertise leads some boards to heavily rely on the chief information security officer (CISO) to coach them on cybersecurity concepts, risks, program objectives, and even the process of cybersecurity oversight itself.
>
> Our interviews suggest that without expertise, directors are less likely to perceive CISOs giving self-serving reports (e.g., by filtering or obfuscating information) to be a barrier to cyber risk assessment and oversight, whereas expert directors, consultants, and even CISOs widely believe this to be an important issue.
>
> In addition, inexpert directors are less able to detect when CISOs filter reports and their oversight of cybersecurity risk generally lacks independence.
>
> In contrast, expert directors perceive improvements in oversight effectiveness

> when boards have genuine cybersecurity expertise, and this view is also shared by CISOs and consultants. **Overall, we conclude that when boards have cybersecurity expertise, they are more likely to provide substantive oversight, as expected under agency theory.**[16]

In summary, directors with cybersecurity expertise strengthen the boardroom as a control in ways not possible without director cybersecurity expertise, which leads to stronger cybersecurity systems. This outcome is rational, logical, and repeatedly proven.

Since the finalization of the SEC cybersecurity disclosure rules in 2023, the importance of director cybersecurity expertise has only become more glaringly apparent and needed. America's chronic cybersecurity issues won't be solved until the boardroom cybersecurity leadership weakness is addressed as a matter of governance policy priority.

Boardroom leadership on cybersecurity adds value. From setting the cybersecurity tone at the top of the organization to building a culture of cyber resilience to being an effective leadership control that strengthens management's cybersecurity system, to more effectively protecting investor interests from this dynamic and challenging business risk. There is no mitigation for the lack of director cybersecurity expertise in the boardroom.

With cybersecurity risks guaranteed to continue and expand, America's boardroom leadership can no longer continue to be a passive and symbolic observer in building and maintaining a resilient cybersecurity system.

In originally excluding this provision from the Final Rules, the SEC explained its rationale as follows, which evidence and the compounding complexity of these and new technologies, such as AI, have since invalidated:

> Directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise.[17]

The evidence has shown this not to be the case — the lack of director cybersecurity expertise creates cybersecurity risk and weakness, and generalist director competencies are ineffective at governing cybersecurity risk.

Business risk has never been a generic concept; it is always contextual to a particular technology, issue, or objective being pursued. In addition, the prior evidence from those working with corporate boards or within the boardroom supports the reality of cybersecurity risk being a unique and complex risk that

needs domain expertise to govern effectively. Cybersecurity risk is not a general concept capable of being effectively governed by the generalist, accounting, and financial-centric strengths of many existing corporate directors.

In the public commentary solicitation related to the proposed cybersecurity disclosure rules, there were additional arguments presented to the SEC in 2023, both FOR and AGAINST director's cybersecurity expertise disclosure. Evidence and reality have invalidated the arguments presented AGAINST director cybersecurity expertise disclosure, while reinforcing and validating the arguments presented FOR director cybersecurity expertise disclosure.

There was support FOR and AGAINST the director cybersecurity disclosure rules from two very different groups of advocates. The FOR camp was represented by associations and companies with deep applied cybersecurity expertise and a vested interest in reducing cybersecurity risk. The FOR camp included cybersecurity associations and leading cybersecurity software companies, institutional investors and their associations, the AICPA, and independent academic research that backed up their conclusions with proof, i.e., collectively those who understand the complexity of cybersecurity and who ultimately bear the risk.

The AGAINST camp was comprised primarily of corporate governance associations that lack expertise in cybersecurity, together with a fairly random and large collection of industry groups, some law and accounting firms, and the NYSE. They share a lack of deep applied knowledge and expertise in cybersecurity. Notably, by default, cyber adversaries would also be in the AGAINST camp as they have a vested interest in keeping boardroom leadership weak on cybersecurity.[18]

Absent a reversal of the SEC's original retraction of the director cybersecurity expertise disclosure rule in the Final Rules, the SEC will also, by default, continue to advance the interests of America's cybersecurity adversaries, at the expense of investors and other stakeholders.

While the hackers are clearly in the AGAINST camp as they have a vested interest in keeping cybersecurity leadership weak within America's companies, the opinions and arguments presented AGAINST the proposed director cybersecurity expertise disclosure rule were evidence-free and fell into a common group of fallacies that could be described as promoting fear, uncertainty, and doubt.

The arguments AGAINST the common sense and simple director cybersecurity expertise disclosure provision were analyzed and found to reflect one or more of five fallacies that were free of evidence, alarmist, and have since been proven unjustifiable:

THE ONE SIZE FITS ALL FALLACY – This false claim stated that the SEC proposed rule defined and dictated one approach for all companies for what constitutes a director with cybersecurity expertise; it did not. The proposed rule does not require director cybersecurity expertise to be added to the board, nor narrowly define director cybersecurity expertise, which provides significant issuer flexibility and the option to make their own decisions if director cybersecurity expertise is needed.

THE ONE-TRICK PONY FALLACY – This fallacy was a dismissive effort to pigeonhole CISOs, or potential director cyber experts, as "specialists" with skills and capabilities that are too narrow to contribute to the broader boardroom and business agenda.

This fallacy demonstrates a lack of understanding of the CISO role that fails to reflect the specific and general business competencies possessed by these business executives that complement their deep understanding of cybersecurity technology and risk, and how digital business systems drive value within the organization. The CISOs who are already joining the corporate boardroom are proving to be valuable contributors to directorship in cybersecurity and beyond.

THE SCARCITY FALLACY – This claim attempted to dismiss the director cybersecurity disclosure issue outright with the claim that there are not enough qualified director cyber experts to go around in the boardroom, so why even bother with disclosure?

Reality has proven that there are many boardroom-qualified technology experts with cybersecurity expertise both willing and capable, some of whom are already succeeding as high-performing corporate directors. And more are willing and able to serve every day. Moreover, many are actively developing their capabilities for directorship as they spend more time with their own boards and begin to actively pursue directorship.[19] As lifelong learners with well-developed cross-functional teaming skills, amongst other core competencies valuable in the boardroom, cybersecurity executives have had to adapt throughout their careers to the constant evolution of information systems and how those systems impact business value, making them particularly well suited to the changing and volatile dynamics of corporate directorship and the modern business.

THE SLIPPERY SLOPE FALLACY – This evidence-free claim attempted to create fear, uncertainty, and doubt that director cybersecurity expertise disclosure or the presence of such a director on the board would create a wide range of negative unintended consequences from a governance perspective or beyond.

Experience has shown that director cybersecurity expertise on the board works to strengthen the cybersecurity system, and the unintended consequences are positive ones,

including how cybersecurity expertise in one or more directors builds cybersecurity literacy levels amongst all directors, through informal peer learning and engagement

THE OUTSIDE EXPERT FALLACY – This mistaken belief proposes that outside experts or management expertise is a suitable replacement for corporate governance, which fails to recognize the board's legal responsibilities and directors' fiduciary duties. Evidence has also proven that the lack of director cybersecurity expertise on the board yields weaker results than when there is director cybersecurity expertise present. Moreover, corporate governance responsibilities cannot be outsourced.

Eighteen months of proof and hindsight have proven that the arguments AGAINST director cybersecurity expertise disclosure were unfounded and groundless. Reality has shown repeatedly that director cybersecurity expertise and leadership in the boardroom work to strengthen the cybersecurity system of America's companies, and the absence of it does the opposite.

By reinstating the director cybersecurity disclosure rule as originally drafted, issuers are not being forced to add this director capability to the board; it is merely a lightweight and easily implemented disclosure requirement. But this will require them to critically consider this issue and to be actively accountable and transparent with investors for their decision, a critical leadership control issue in cybersecurity that investors deserve clarity and transparency on, given the material business risks of cybersecurity.

THE CYBERSECURITY RISK LANDSCAPE IS SHIFTING AND BECOMING MORE COMPLEX

Since the implementation of the SEC's Final Cybersecurity Disclosure Rules, which went into effect on December 15, 2023, cybersecurity risk and its negative impacts have continued to escalate faster than cybersecurity controls and mitigations. The lack of boardroom cybersecurity leadership and expertise is a key contributor to this expanding gap.

We believe the SEC should remedy its prior decision, and lead by strengthening the boardroom as a cybersecurity control by reinstating the proposed director cybersecurity expertise disclosure rule, given the rapidly escalating and changing cybersecurity risk environment.

The Proposed Rule is a common-sense, easily implemented, and high ROI disclosure provision that will lead to the material strengthening of each company's cybersecurity system, directly benefiting investors and other stakeholders, including America's overall economic system. A growing body of evidence supports this.

Cybersecurity risk is not a static risk; it constantly evolves. Even in the 18 months since the inception of the Final Rules, cybersecurity risks have materially changed. This type of environment and its dynamic pace requires director cybersecurity expertise to understand and effectively govern over the short- and long-term. The following issues are contributing to the rapid escalation and expansion of the cybersecurity risk environment facing American businesses, and the need for the SEC to reverse this prior decision:

1. **Cybersecurity risk is growing as America, and its businesses, remain one of the world's highest priority cybersecurity targets**[20] — The lack of cybersecurity expertise and leadership in the boardroom perpetuates a material cybersecurity leadership control weakness throughout America's economy, allowing the cybersecurity risk gap to expand uncontrolled, and materially jeopardizing investor interests. This chronic weakness keeps America as a highly attractive and vulnerable target for adversaries.

2. **Artificial Intelligence technologies are introducing new systemic cybersecurity risks and arming adversaries with new tools that are expanding America's cybersecurity resiliency gap** — America's cybersecurity resiliency and defenses need to both keep up and be hardened against these expanding risks which requires the boardroom to be an effective control, which only occurs with the presence of director cybersecurity leadership and expertise.

3. **The Federal government is reducing its resource commitment to cybersecurity however, the risk landscape continues to expand** — This places a greater burden on the private sector, which mandates effective private-sector cybersecurity leadership that must start in the boardroom.

4. **Systemic cyber risk is increasing with AI and generally with other digital developments, where one company's cybersecurity weakness can create risk for many other companies** — The board needs to more effectively govern this challenging dimension of cybersecurity risk, which requires more than symbolic oversight. It needs the depth of understanding that director cybersecurity expertise brings to understand and monitor the complex and distributed nature of cybersecurity risk.

5. **Non-compliance with the Final Cybersecurity Disclosure Rules has been rampant, primarily with Section 1.05 regarding incident disclosure and incident impacts**[21] — This non-compliance demonstrates the lack of maturity of many companies' key processes in cybersecurity, including the basic process of understanding cybersecurity incident impacts in the context of investor interests. This illustrates why the cybersecurity disclosure rules were needed in the first place, and why stronger and more effective boardroom cybersecurity leadership and

experts are needed who can ensure that the cybersecurity system operates at a foundational and functional level and that existing SEC Rules are appropriately understood and applied.

6. **The European Central Bank (ECB) has established a regulatory precedent in the banking sector with the requirement for boards across Europe to have directors with cybersecurity expertise, and NIS2 is raising standards for the board's role in cybersecurity across Europe**[22] — ECB regulation of this leading practice strengthens every company within the EU banking system. It's an example of the regulatory leadership needed that will strengthen the entire EU banking system over this critical boardroom cybersecurity leadership control weakness. America should be a leader in cyber resiliency, not a laggard, especially in the boardroom. America will always underperform in cybersecurity until the boardroom cybersecurity control weakness is addressed. Adversaries target weakness, and as others strengthen their cybersecurity systems, this encourages adversaries to attack those who remain weak.

   The EU directive known as NIS2 has also raised its standards that strengthen the role and capability of the boardroom in governing cybersecurity risk across the EU. These new requirements embody clear expectations for the management body, i.e., the board, of EU member companies to explicitly approve the cybersecurity risk management programs, and that they can be held liable for these actions. They are also explicit in the expectation that board members receive training that strengthens their cybersecurity literacy and expertise levels, such that they have sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk management practices and their impacts on the organization.[23] Fulfilling these requirements requires director-level cybersecurity expertise.

   Both of these leading regulatory initiatives are strengthening corporate boards and their directors as active and effective leadership controls, not symbolic ones.

CONCLUSION

Reinstating the director cybersecurity expertise disclosure requirement as previously drafted will encourage and incentivize issuers to actively address this vital cybersecurity leadership control weakness, and many of them will undoubtedly add this long overdue director capability to the board, strengthening their cybersecurity systems in the process.

Disclosure of their approach to this critical boardroom cybersecurity control is material information for investors in assessing the risk profile of their investments. Reality also demonstrates that a director with cybersecurity expertise reduces cybersecurity risk.

With the prior elimination of the director cybersecurity expertise disclosure provision from the SEC Final Cybersecurity Disclosure Rules, the boardroom cybersecurity leadership control is guaranteed to remain a weak link in most companies' cybersecurity systems, ensuring that America's cybersecurity risk profile is much weaker than it should and could be.

We encourage the SEC to reverse its prior decision and to reinstate this common-sense disclosure provision to lower America's cybersecurity risk profile and strengthen the American economy with cybersecurity leadership that starts at the top of American business.

While the leading practice of boards adding director cybersecurity expertise is a practice that slowly continues to grow through self-regulated leadership from responsible and informed boards, a more rapid universal strengthening of the boardroom as a cybersecurity leadership control is needed. SEC regulatory reinstatement of the proposed rule will deliver this as it will establish director cybersecurity expertise as a leading practice standard in America's public company boardrooms.

As one of the world's most consistently targeted countries for cybersecurity adversaries, American businesses and their boardrooms should set the standard for leading practices in cybersecurity governance, strength, and resilience, not lag behind them. Today, America significantly lags in boardroom cybersecurity leadership and effectiveness.

Boardroom cybersecurity leadership needs strengthening within every boardroom, given that one company's cybersecurity weakness can create systemic risk and far-ranging impacts for many other companies and the larger American economy. This "tragedy of the commons" dynamic requires a solution that only a collective regulatory intervention can deliver. This will strengthen America's economy and its cybersecurity "commons," which are facing a higher risk profile than they should be, to help ensure that America's companies can successfully and securely navigate their path into the digital future.

The evidence and market conditions justify our Petition for reinstatement of the proposed rule for director cybersecurity expertise disclosure, and we make this request.

Specifically, we request that the SEC reinstate the proposal to amend Item 407 of Regulation S-K to require disclosure regarding the cybersecurity expertise of members of the board of directors, if any. This Proposed amendment would have also required the name(s) of such individual(s) along with a description of the nature of their cybersecurity expertise, which we also support. We recommend adopting the Rule as drafted in the Proposing Release.

Thank you for your attention to this request, and we are pleased to discuss our views with you. Please contact me directly at bob@digitaldirectors.network if you would like to discuss these views.

Sincerely,

Bob Zukis
Founder and CEO
Digital Directors Network
www.digitaldirectors.network

/s/ Robert Huber
Chief Security Officer, Head of Tenable Research, President of Tenable Public
Tenable Holdings, Inc. (Nasdaq: TENB)
www.tenable.com

/s/ Bob Ackerman
Founder, Chairman & Managing Director
Allegis Cyber Capital
www.allegiscyber.com

/s/ Patrick Gaul
Executive Director
National Technology Security Coalition
www.ntsc.org

/s/ Kevin Richards
President, Cyber Risk Solutions
X-Analytics
www.x-analytics.com

/s/ Valmiki Mukherjee
Founder & Chairman, Cyber Future Foundation
CFF - Professional Association of CISOs
www.cyberfuturefoundation.org

/s/ Jimmy Sanders
President of ISSA International
Information Security Systems Association
www.issa.org

/s/ Bartlett Layton
Chief Executive Officer
AI Guardian
www.aiguardianapp.com

/s/ Malcolm Harkins
Chief Security & Trust Officer
Hidden Layer
www.hiddenlayer.com

/s/ Kasi Paturi
President
Pan Asian American Business Council
www.paabc.org

Endnotes

[1] U.S. Securities and Exchange Commission (SEC). (2023, August 4,). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure FINAL RULE (2023-16194; 88 FR 51896; Release No. 33-11216, 34-97989 File No S7-09-22). https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

[2] U.S. Securities and Exchange Commission (SEC), (March 23, 2022) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure PROPOSED RULE (2022-05480; 87 FR 16590; Release No. 33-11038; 34-94382; IC-34529; File S7-09-22) https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

[3] Digital Directors Network is the leading boardroom learning network exclusively focused on developing the practice and profession of digital and cybersecurity governance. With over 1,600 IT, cybersecurity and boardroom members, we are at the forefront of developing and applying leading practices that strengthen the role of the boardroom as a control in shaping and securing the digital future.

[4] Tenable exists to expose and close priority security gaps that put businesses at risk. By protecting digital and critical infrastructure from exposures, Tenable reduces business risk for more than 44,000 customers around the globe.

[5] AllegisCyber Capital is the pioneer in VC investing in cybersecurity. Founded by experts in the field of cybersecurity over two decades ago, Allegis is at the forefront of issues and solutions reducing cybersecurity risk.

[6] X-Analytics is the worldwide leader in helping boards and companies understand their business exposure to cyber risk, so they can implement effective mitigation strategies that reduce risk to create investor value.

[7] The Cyber Future Foundation was established to create a brighter and trusted future for the cyberspace where digital commerce and innovation can thrive based on trust and respect for individual privacy.

[8] As a non-profit, non-partisan organization, the National Technology Security Coalition (NTSC) serves as the preeminent advocacy voice of the CISO and brings US Government and industry cybersecurity leaders together to network and solve today's cybersecurity policy and collaboration challenges. Comprised of CISOs from Fortune 1000 companies and academic institutions from across the United States, our membership represents a wide cross-section of industries—sharing experiences, expertise, and ideas as they collaborate on issues of national importance to the CISO.

[9] HiddenLayer is a cybersecurity company specializing in protecting artificial intelligence (AI) and machine learning (ML) models from adversarial threats.

[10] The mission of the Pan Asian American Business Council ("PAABC") is to enable and foster the development and growth of Asian American owned businesses

[11] AI Guardian provides an enterprise-grade platform that enables organizations to govern AI systems with confidence - offering automated risk assessments, compliance management, and oversight of third-party AI tools to ensure transparency, accountability, and regulatory alignment.

[12] The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners with over 7,500 members.

[13] Ibid., n. 2. pp. 44-46 Original footnotes excluded.

[14] Dave DeWalt. 2024. State of Cyber Awareness in The Board Room Report, Night Dragon and Diligent Institute

[15] Michelle Lowry, Marshall Vance, Marshall, Anthony Vance, (2022) Re: S7-09-22 Cybersecurity Risk Management, Strategy, Governance (RSG), and Incident Disclosure, Virginia Tech, Pamplin College of Business,

[16] Michelle R. Lowry; , Anthony Vance, Marshall D. Vance; (2025) Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity. Management Science

[17] Ibid., n. 1, p. 85

[18] Bob Zukis. (2024). The DOMINO Guide: The Definitive Boardroom Guide on Digital, Cybersecurity and Systemic Risk Governance. Digital Directors Network, DDN Press.

[19] Digital Directors Network has been recruiting, developing and certifying CIOs and CISOs and directors on digital, cybersecurity and general corporate governance through a widely acclaimed executive education masterclass program since 2019.
[20] Check Point Research. April 16, 2025. Q1 2025 Global Cyber Attack Report from Check Point Software: An Almost 50% Surge in Cyber Threats Worldwide, with a Rise of 126% in Ransomware Attacks. https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/
[21] Sheresse Smith, Michelle Reed, Aaron Charfoos, Dave Coogan and Jeremy Berkowitz, (December 2024), SEC Cybersecurity Incident Disclosure Report, Paul Hastings
[22] European Central Bank, February 21, 2024, "Supervision Newsletter: New Policy for More Bank Board Expertise in UICT and Security Risks," https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2024/html/ssm.nl240221_2.en.html
[23] European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union L333 (December 27, 2022): 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj.