U.S. CYBERSPACE SOLARIUM COMMISSION
POTOMAC GATEWAY SOUTH
2900 CRYSTAL DRIVE, SUITE 250
ARLINGTON, VA 22202

May 7, 2020

The Honorable Jay Clayton
Chairman
Securities and Exchange Commission
100 F St NE
Washington, D.C. 20549

Dear Mr. Clayton,

We write to you in our capacities as the commissioners of the Cyberspace Solarium Commission (CSC) to encourage the Securities and Exchange Commission (SEC) to exercise its authority under Section 404 of the Sarbanes Oxley Act of 2002 (SOX) to require reporting on cyber risk. The CSC was created by Congress in the 2019 National Defense Authorization Act as a bipartisan, public-private body to develop a strategic approach to defending the United States in cyberspace against cyber incidents of significant consequence. The fourteen commissioners include four legislators, four senior executive agency leaders, and six nationally recognized experts from the private sector. Our report focuses on a strategy of *layered cyber deterrence* and includes more than 80 recommendations on ways to implement that strategy.

One of our recommendations, Enabling Recommendation 4.4.4, pertains to SOX. We recommend the SEC more strenuously mandate reporting and assessment of cybersecurity controls on financial reporting, and we believe it currently has the authority to do so. Under Section 404 of SOX, companies are responsible for "establishing and maintaining an adequate internal control structure and procedures of financial reporting."[1] Further, the SEC's rules state that the required reporting related to the internal control over financial reporting (ICFR) should "pertain to the maintenance of records… [and] provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements."[2] SEC guidance issued in 2007 stated that "[m]anagement's evaluation of the risk of misstatement should include consideration of the vulnerability of the entity to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets and corruption), and whether any such exposure could result in a material misstatement of the financial statements."[3]

Additional SEC guidance issued in 2018 stated that rules requiring "a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures" and rules requiring "companies to disclose conclusions on the

[1] 15 U.S.C. § 7262
[2] 17 C.F.R. §240.13a–15(f)
[3] Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, Release No. 33-8810 at 14 (Jun. 27, 2007).

effectiveness of disclosure controls and procedures," including the final rule adopted under Section 302 of the Sarbanes-Oxley Act of 2002, "should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact."[4] In particular, the 2018 guidance notes that "to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective." We appreciate this guidance, which built upon the 2011 staff guidance related to cybersecurity. However, we note that for virtually any publicly traded company, cybersecurity risks and incidents *do* pose risks to its ability to record and report financial information, and the SEC must help companies understand how to evaluate whether deficiencies exist in their cybersecurity controls.

In a time when cyber threats are increasingly common and sophisticated, now is the time for the SEC to specifically lay out the responsibilities issuers have to address cyber risks in attestations made under Section 404 and to engage in enforcement actions as needed to ensure these requirements are followed.

Accounting for Cyber Risk as Part of ICFR

Today, most if not all companies keep their financial records electronically. Company executives and external auditors must have a full understanding of how those electronic records are protected if they are to attest to their accuracy. Threat actors targeting vulnerabilities in information and communications technology can disrupt the internal control structure for financial reporting by affecting the integrity of electronic records.

The Public Company Accounting Oversight Board (PCAOB) has articulated concerns that cybersecurity incidents are a risk that could prompt a material misstatement of financial statements.[5] While the PCAOB notes that none of the cybersecurity incidents it reviewed in 2016 were related to material misstatements of financial reporting, risks exist that future cyber incidents may affect issuer financial statement reporting.[6] Indeed, a recent example demonstrates how a cyber incident could cast doubt on the accuracy of financial data. Last year, a malware incident affecting Dutch accounting software firm Wolter Kluwer caused many accountants from US firms to have difficulty accessing their clients' financial data from the software company for several days.[7] The targeting of the firm, which, according to its website, serves 92 percent of the world's top 50 banks and many Fortune 500 companies, sparked concern about the security of financial information stored on its servers and caused a "quiet panic" among its clients.[8]

---

[4] Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018).
[5] PCOAB Staff Inspection Brief "Preview of Observations from 2016 Inspections of Auditors of Issuers;" Vol 2017/4 (November 2017).
[6] PCAOB Standing Advisory Group Meeting; Panel Discussion- Cybersecurity (June 5-6, 2018); https://pcaobus.org/News/Events/Documents/Cybersecurity%20Briefing%20Paper.pdf
[7] Fazzini, K. (2019, May 9). A malware attack against accounting software giant Wolters Kluwer is causing a 'quiet panic' at accounting firms. Retrieved from https://www.cnbc.com/2019/05/08/wolters-kluwer-accounting-giant-hit-by-malware-causing-quiet-panic.html
[8] *Ibid*.

An additional type of risk to the accuracy of financial data is that companies may report financial data at a time when their systems have already been breached but before they are aware of such a breach. While there may be cases where a reasonable company could not be expected to know their networks have been penetrated, in many cases, commonly used network monitoring tools would allow a company to know it had been breached and adjust its financial statements accordingly.

A 2019 IBM study estimated that companies take 206 days on average to simply detect a data breach, up from 197 days in 2018 and 191 in 2017.[9] In the well-known Equifax breach in 2017, for example, Senate investigators found that a combination of inadequate and negligent security practices allowed cyber attackers to penetrate and maneuver undetected within Equifax's networks for 78 days. Moreover, the company did not publicly disclose the breach for almost four months.[10] In the time between the initial breach and Equifax's discovery of the breach, the company made three filings that reported financial information that would significantly change after discovery of the breach. Failing to detect a network intrusion due to a company's poor cybersecurity practices does not absolve a company of its responsibility under Section 404 to report accurate financial data. In fact, the ability to detect breaches in a timely manner is an essential quality of an "adequate" system for maintaining internal control over financial reporting.

Defining Internal Cyber Controls

Should the SEC, as the CSC recommends, issue guidance clarifying that cyber threats pose a risk to ICFR, the SEC may need to issue new rules and guidance outlining what "adequate" internal control structures look like to mitigate cyber risk.

The CSC does not support a "one-size-fits-all" approach to risk management. Not every vulnerability is equally critical, nor is every security control appropriate for every issuer subject to Section 404 requirements. Through the work of the CSC, we found the use of risk management frameworks, such as the National Institute of Standards and Technology (NIST) "Cybersecurity Framework,"[11] to be of significant benefit.

However, many implementations of risk management frameworks rely on qualitative assessments (e.g., "Framework Implementation Tiers" in the NIST model). While these qualitative approaches can prove useful in helping organizations understand how they approach cyber risk, they are not sufficient to determine whether an organization's risk management decisions are "adequate." In addition, we urge the SEC to consider how *risk quantization* can help an entity to accurately report its desired level of cyber risk and to determine whether its controls are adequate to achieve that level of risk.

In issuing guidance or conducting rulemaking related to the evaluation of the potential impact of cyber risk on ICFR, therefore, the SEC should set clear expectations regarding the use of risk

---

[9] IBM and Ponemon Institute, 2019 Cost of a Data Breach Study, USA, 2019.
[10] United States Congress, Senate Committee on Homeland Security and Government Affairs, Permanent Subcommittee on Investigations (March 2019). *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach*.
[11] https://www.nist.gov/cyberframework

quantization in demonstrating the adequacy of ICFR. Furthermore, in conducting the annual assessment required under Section 404, the SEC should also require the use of risk quantization and an explanation of data sources (e.g., the results of internal penetration tests) used to validate the effectiveness of ICFR.[12]

The CSC further requests, in the event the SEC does not agree with our perceived need for additional guidance in this area, that the SEC share its rationale with us. We believe understanding the SEC's reasoning and approach to the issues we have highlighted would help the various stakeholders identify and implement other potential measures to effectively quantify the cyber risk to their ICFR.

Conclusion

In our work with the CSC, we found raising cybersecurity standards among the private sector to be imperative given the pervasive and constantly evolving nature of cyber threats. We believe that an assessment of a firms' financial controls is incomplete without accounting for cyber risk and that, therefore, the SEC's existing responsibilities under Section 404 of SOX demand the development of additional guidance or rules clarifying what issuers must do to account for such risk. To determine whether an internal control structure is "adequate" and to assess its control "effectiveness" – both determinations required under Section 404 – issuers should attempt to quantify the cyber risk to the integrity of their ICFR.

We urge the SEC to address these concerns by issuing specific guidance or conducting further rulemaking under Section 404 to incorporate the assessment of cyber risks.

Moreover, we encourage the SEC to more rigorously *enforce* any cyber risk rules related to Section 404. We note that, since 2011, the SEC has promulgated guidance requiring companies to disclose "material" cyber risks to shareholders, but both the 2011 and 2018 guidance would be more effective if backed up by regular enforcement actions. The 2018 reissued interpretive guidance states that "although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, companies nonetheless may be obligated to disclose such risks and incidents."[13] Yet companies still overreport small cyber events and underreport large ones, making the disclosures less valuable. Under Section 404 of SOX, the SEC has the responsibility to spell out, obligate, and enforce disclosure of cyber risk as it relates to ICFR. Enforcement is a key driver of desired behavior.

The CSC firmly believes that there is more than adequate justification for immediate SEC action and that existing risk quantization approaches could help issuers to comply with new guidance or

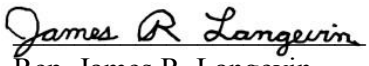
[12] Cybersecurity risk quantization frameworks exist and are already being used in industry and government. For instance, The Open Group Standards for Risk Analysis and Risk Taxonomy, based on the Factor Analysis of Information Risk™ standard, provides a common taxonomy and methodology for the quantitative modeling of information security and operational risk, as do other cyber "Value at Risk" models. In a separate recommendation (4.3), the Commission recommends the establishment of a Bureau of Cyber Statistics to help develop better metrics to use as inputs for such models.

[13] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746 (February 26, 2018).

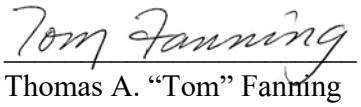
rulemaking. We would welcome the opportunity to discuss this issue further with you and your staff if you have questions about our proposal.

Our report notes: "The more digital connections people make and data they exchange, the more opportunities adversaries have to destroy private lives, disrupt critical infrastructure, and damage our economic and democratic institutions." Our whole-of-nation approach to counter those adversaries demands more of our government and our private sector. We hope you will join us in our mission to make cyberspace more secure.

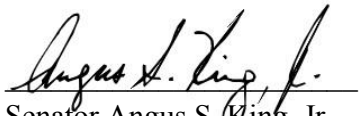
Sincerely,



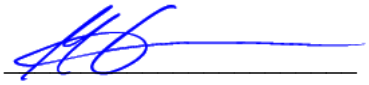
Rep. James R. Langevin
Commissioner



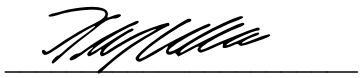
Thomas A. "Tom" Fanning
Commissioner



Senator Angus S. King, Jr.
Co-Chairman

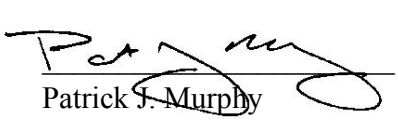


Rep. Michael J. "Mike" Gallagher
Co-Chairman

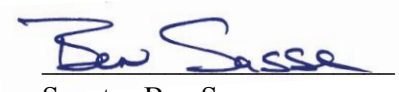


Frank J. Cilluffo
Commissioner

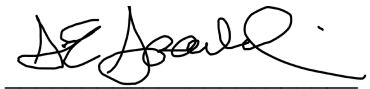
John C. "Chris" Inglis
Commissioner



Patrick J. Murphy
Commissioner



Senator Ben Sasse
Commissioner



Suzanne E. Spaulding
Commissioner

Dr. Samantha F. Ravich
Commissioner

cc: The Honorable Hester M. Pierce, Commissioner, SEC
The Honorable Elad L. Roisman, Commissioner, SEC
The Honorable Allison Herren Lee, Commissioner, SEC