May 9, 2022

Submitted electronically via SEC.gov

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

[Submitted via email to rule-comments@sec.gov]

Dear Ms. Countryman:

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

BuildingCyberSecurity.org[1] (BCS) is a global non-profit organization established in 2020 to establish and sustain cyber protection **performance** frameworks developed by stakeholders across multiple sectors offering market-driven options and insurance incentives to mitigate cyber risk in connected networks, controls, and devices in an increasingly smart world. The BCS framework is improving human safety globally by incentivizing investments in protected operational technologies (OT), related information technology (IT) networks, processes, training, and recovery plans to enhance the security of cyber-physical systems against rapidly evolving threats in technologically advancing societies. The BCS framework is being used by asset owners and insurers to assess cyber-related exposure, and to certify various levels of continuous monitoring, validation, and improvement of cyber protections to respond to a rapidly evolving threat based on a company's internal risk management framework. Our goal is to offer companies a return on cyber protection investments to mitigate risk by favorable consideration in the development of insurance policy terms for a wide range of risk transfer instruments (cyber, property, casualty, directors/officers, technical omissions, etc)

BCS represents a broad group of private and public stakeholders, including cyber security experts, system manufacturers and integrators, asset owners/managers, cyber security companies, insurers, designers, and engineering companies committed to a comprehensive IT and OT cyber protections in a framework that will consistently evolve and mature to meet rapidly moving cyber threats. A private sector framework bases on industry best practices is more responsive, flexible, and effective that government standards that lag 2-4 years behind the threat.

Perspective on the Proposal

BCS strongly supports adoption of Item 106(b) and (c). Publicly traded companies face an unprecedented existential threat where asset or brand value, business operations, reputation and safety for employees and customers can be threatened or disrupted with one keystroke in a matter of minutes. The billions of cyber attack vectors from Nation States and terrorist organizations to criminal actors, cyber hackers, and even disgruntled employees or customers present an overwhelming risk for most companies relying on the internet, networks or connected

[1] https://buildingcybersecurity.org/

devices and infrastructure for their revenue. The SEC must take action now to raise the priority of remedies and investments to protect operations. Requested input is submitted as follows:

Input to question 16 Are there other aspects of a registrant's cybersecurity policies and procedures or governance that should be required to be disclosed under Item 106, to the extent that a registrant has any policies and procedures or governance?

BCS strongly recommends the study and inclusion of the need to cite or measure cyber performance against a standard reference architecture or framework to allow registrants to qualify the efficacy and implementation of their policies, including the use of third-party assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program. Existence of a cyber program is not as important to investors/shareholders as its performance. Asking a registrant to report the existence and brief description of a cyber security program without a national framework or reference architecture results in management and boards of directors guessing at "effective" or "reasonable" strategies to address cybersecurity risks. This concern is the source of lawsuits where business disruptions have resulted in significant economic loss. "Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and "reasonable" measures to ensure that the Pipeline's critical infrastructure was safeguarded," [2] Many industries already have specific regulations for cyber security programs and metrics. An example would be Critical Infrastructure Protection standards for utilities developed by the North American Electric Reliability Corporation, a non-profit body created and funded by the utilities themselves and subject to the Federal Energy Regulatory Commission, the United States government's regulatory entity for energy. Other industries are developing new cyber guidance through trade associations or other organizations. Certain industries rely on meeting federal standards developed by the National Institute of Standards and Technology (NIST). BCS has developed a framework of protections for the commercial real estate industry. Bottom line, investors must be able to assess a registrant's cyber programs and governance against what has been adopted as a reasonable standard for their industry.

In addition, in a connected, smart society, cyber threats are constantly evolving, metastasizing, and expanding with millions of new attack vectors added each day. We recommend that Item 6 include a description how a company's policies and governance assess the "reasonable" future likelihood and impact to the registrant's results of operations or financial condition with intelligence or updated information on emerging cyber methods and trends. Boards can no longer rely on static audits conducted annually to assess cyber risk. Dynamic real-time monitoring, feedback, and security actions at the speed of relevance within a performance framework will be more effective for companies to mitigate future risk.

Input to question 19. **The proposed rule does not define "cybersecurity." Would defining "cybersecurity" in proposed Item 106(a) be helpful? If defining this term would be helpful, is the definition provided above appropriate, or is there another definition that would better define "cybersecurity"?**

[2] https://topclassactions.com/lawsuit-settlements/money/colonial-pipeline-says-it-has-no-obligation-to-reimburse-consumers-after-ransomware-attack/

BCS believes adopting a definition for "cybersecurity" in Item 106(a) would be helpful for corporate boards to establish a standard understanding of the risk across all functions of a company in order to determine the cyber expertise required on the Board. BCS defines cybersecurity as "any action, step, or measure to detect, prevent, deter, mitigate, or address an attempt to gain unauthorized access to, and exploit software or hardware for purposes other than intended by the owner, and to ensure confidentiality, integrity, and availability of information and operations."

In this definition, BCS specifically addresses hardware (microchips, process logical controllers, sensors, industrial controls systems, operational technologies, smart devices, etc) as a distinct cyber security concern for companies and shareholders. A cyber attack on hardware for a company would have different effects, including threats to human safety, health, and property or in certain cases, a threat to the essential services society relies on for existence. A perfect example would be the ransomware attack in May 2021 on the Colonial pipeline, which quickly escalated from a seizure/encryption of data systems to the closure of part of the east coast fuel supply due to concerns about migration of the attack into OT systems and the severing of automated smart meters from the IT systems that had been seized. For publicly traded companies which rely on connected or automated OT for asset or operational performance (commercial real estate, manufacturing, healthcare, transportation, robotics, critical infrastructure, etc), a threat to those systems would have an immediate and asymmetrical impact on a company's value.

The President of the United States, with the support of the Cybersecurity and Infrastructure Security Agency (CISA), has published numerous National Security memorandum[3], alerts[4], and guidance[5] in the last year specifically addressing the unique risk in cyber-physical systems. (CPS). We recommend that disclosure of policies and procedures, to identify and manage cybersecurity risks and threats, include governance, policies and procedures, or technologies to mitigate physical or other harm to employees or customers, reinforcing the determination by federal agencies of the unique cyber risk to human safety.

Input to question 20**. Should we require the registrant to specify whether any cybersecurity assessor, consultant, auditor, or other service that it relies on is through an internal function or through an external third-party service provider? Would such a disclosure be useful for investors?**

BCS experts contend that specifying the cybersecurity assessor, consultant, auditor, or other service, internal or external, may create more harm than good. Instead, investors would benefit more from knowing the benchmarked results of the actions measuring investments and outcomes to mitigate cyber risk against a national reference architecture, standard, or industry-developed framework.

Conclusion

[3] https://www.cisa.gov/control-systems-goals-and-objectives
[4] https://www.cisa.gov/uscert/ics/alerts
[5] https://www.cisa.gov/uscert/ics/Recommended-Practices

BCS commends the SEC for this important initiative to address the #1 corporate risk globally, and more importantly, a societal existential risk that can detrimentally impact lives in a matter of minutes if we fail to implement safeguards and protections in a cyber connected world. We stand ready to work directly with the Commission as it moves forward to develop a clear, transparent, and effective set of cybersecurity disclosure rules. Should you have questions or require additional information, please contact Lucian Niemeyer, Chief Executive Officer, BuildingCyberSecurity by telephone at [redacted] or by email at [redacted].

Thank you for the opportunity to comment on this important issue.

Respectfully submitted,

Building Cyber Security.org