January 3, 2022

Mr. Gary Gensler
Chairman
Securities and Exchange Commission 100 F St NE
Washington, D.C. 20549

Dear Mr. Gensler,

We are the members of the Board of Directors, Advisory Board, and Leadership Team of the FAIR Institute, an expert, non-profit organization led by cybersecurity and operational risk professionals to develop and promote better risk management practices through the financial quantification of risk. The Institute counts over 12,000 members representing 45% of the Fortune 1,000 Companies and 25 U.S. Federal Government Agencies. The FAIR Institute was named one of the "Most Important Industry Organizations of the Last 30 Years" at the 2019 SC Media Awards.

Over the past years, we have had the privilege to connect and work with the members of the Cyberspace Solarium Commission (CSC). Representatives Jim Langevin (D-RI) and Mike Gallagher (R-WI), co-chairs of the Commission and Chris Inglis, National Cyber Director, have spoken at our annual FAIR Conference in the past. They all echoed the recommendation of the CSC to improve the assessment and disclosure of material cyber risks by large organizations through the financial quantification of risk, as a critical means to better understand the impact of cybersecurity events and to determine the adequacy of risk mitigation measures. After all, how can organizations effectively prioritize cyber risk and size mitigation initiatives without understanding its impact on the bottom line?

Following recommendation from the Cyberspace Solarium Commission March 2020 Report, we are encouraging the SEC to require the disclosure of top cyber risks in financial terms as part of Sarbanes-Oxley Audits. The Report states:

"The Sarbanes-Oxley Act was passed in 2002 to improve corporate accountability and oversight in response to a series of corporate failures. The law sets out requirements, enforced through the Securities and Exchange Commission (SEC), for all publicly traded U.S. companies. In 2018, the SEC issued interpretive guidance of existing regulations, stating 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,' including the requirements under Sarbanes-Oxley." [1]

We also would like to acknowledge and endorse a May 2020 letter from the CSC that specifically recommends that the SEC "more strenuously mandate reporting and assessment of cybersecurity controls on financial reporting" under Section 404 of SOX.[2] The full letter, which we support in its entirety, has been attached with this letter as a referenced document.

We agree with the CSC, that cyber risk is now a top business risk. Given this, we firmly believe that the SEC has both the authority and obligation within current regulations, to enforce cyber risk disclosures both pre- and post- any probable cyber loss event. Current guidance only requires risk assessments and disclosure after an incident occurs. Such guidance, right now, does not provide sufficient incentive to proactively assess the materiality of top cyber risks and adopt adequate risk mitigation measures and will continue to result in too many breaches that could have otherwise been prevented. It is time for organizations to push to the next level of maturity, which is to align to a more business-focused approach to cyber. Our experience has

[1] Cyberspace Solarium Commission Report. *A Warning from Tomorrow.* 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

[2] CSC Letter to SEC RE SOX 5.7.2020. https://drive.google.com/file/d/1iwysSUjcqcji6uJ63MykzxnbUl8cGqE8/view

proven, time and time again, that shareholders need reports that communicate the magnitude of cyber risk in terms that they can understand. We have found that communication of the impact of cyber risk in financial terms, in dollars and cents, is the best approach.

Pre-breach audits of financially oriented cyber risk assessments will help organizations better understand the problem they are facing and increase the chances of explicitly implementing adequate risk mitigation measures, as also required by SEC's current guidance on cyber risk.

In your recent testimony to the Senate Committee on Banking, Housing, and Urban Affairs on September 14, 2021, you made the following statements:

"Today's investors are looking for consistent, comparable, and decision-useful disclosures around climate risk, human capital, and cybersecurity. I've asked staff to develop proposals for the Commission's consideration on these potential disclosures."[3]

The consistent and comparable disclosures that you are seeking only exist when companies report them pre-breach. We strongly recommend that the cyber risk disclosure requirements apply to pre-beach audits for public companies. A renewed guidance, along with a requirement to explicitly include top cyber risk assessments as part of Sarbanes-Oxley audits, would greatly improve risk management practices, help protect shareholders and secure our country.

We applaud the work that you and your staff are doing, and we offer our support and expertise as these proposals are being considered.

[3] Gensler, G. (2021, September 14). *Testimony Before the United States Senate Committee on Banking, Housing, and Urban Affairs*. Retrieved November 30, 2021, from https://www.sec.gov/news/testimony/gensler-2021-09-14.

Sincerely,

Jack Jones
Chairman
FAIR Institute

Evan Wheeler
Sr. Director, Technology Risk Management
Capital One

Nicola (Nick) Sanna
President
FAIR Institute

Kim Jones
Director, Security Operations
Intuit

Omar Khawaja
CISO
Highmark Health

La'Treall Maddox
Strategy Risk Manager
Cisco

James Lam
Chair of Risk and Audit Committees,
E*TRADE, NACD 100 Honoree

Sounil Yu
CISO & Head of Research
JupiterOne

Christopher Porter
CISO
Fannie Mae

Jack Whitsitt
Sr. Security Engineer (FAIR / Risk Quantification), Datto, Inc.

Mary Elizabeth Faulkner
CISO
Thrivent Financial

Julian Meyrick
Managing Partner & VP, Security Transformation Services, IBM Security

Wade Baker
Partner and Co-Founder
Cyentia Institute

Andrew Retrum
Managing Director, Global Financial Services Security & Privacy, Protiviti Inc.

Donna Gallaher
President & CEO
New Oceans Enterprises

CC: SEC Commissioners
The Honorable Allison Herren Lee
The Honorable Hester M. Peirce
The Honorable Elad L. Roisman
The Honorable Caroline A. Crenshaw
Jessica Wachter, Director, DERA

Contact Information:
Luke Bader
Director, Membership and Programs
lbader@fairinstitute.org
(484)-885-4144
FAIR Institute
12110 Sunset Hills Road, Suite 573
Reston, VA 20190