BITSIGHT®

May 6, 2022

Via Electronic Submission

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

Re: File No. S7-09-22
Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure

Dear Secretary Countryman:

BitSight Technologies, Inc. ("BitSight") welcomes the opportunity to comment on the Securities and Exchange Commission's ("Commission") proposed rule on cybersecurity risk management, strategy, governance and cybersecurity incident reporting by public companies. We commend the Commission for its attention and focus on this critical issue impacting the investor community and market participants.

Cybersecurity is a critical risk that can materially impact a company's long-term value and sustainability, and increased disclosure will improve the ability of investors and other market participants to assess and price cyber risk. We concur with the Commission that investors would benefit from more timely, consistent and informative disclosure about cybersecurity risks and incidents; further detail about the cyber risk management practices adopted by, and threats facing, individual companies; and additional information about the cybersecurity experience and qualifications of a company's board of directors.

Unfortunately, there are instances where investors today may be in the dark when it comes to understanding the cybersecurity risk posture of the companies in which they invest. Indeed, the frequency and substance of companies' disclosures related to cybersecurity investment, policy, and readiness can vary greatly.[1] Moreover, significant cybersecurity incidents are not always

[1] Recent BitSight research published on March 29, 2022 supports the Audit Analytics analysis referenced by the Commission regarding delays associated with cyber incident disclosures. BitSight analyzed more than 12,000 publicly disclosed cybersecurity incidents from 2019-2022 and found that it takes organizations 105 days to discover and disclose an incident from the date the incident occurred; discovery takes 46 days, disclosure takes 59 days after discovery. This research is available at: https://www.bitsight.com/blog/months-minutes-can-new-regulations-accelerate-cyber-incident-disclosure-process

broadly publicly disclosed, and any disclosures that are provided can lack critical information that would be useful for investors to make informed decisions.[2]

BitSight is a company dedicated to helping investors and other market participants tackle the significant and dynamic challenge of understanding cybersecurity risk. In 2011, BitSight created the world's first cybersecurity rating system and has since partnered with many of the world's leading investment organizations including Moody's, Glass Lewis, IHS Markit, and others to improve investor and market awareness of cyber risks.

BitSight produces daily security ratings and analytics that provide real-time information across a variety of cybersecurity risk factors. BitSight measures the cybersecurity posture of a company based on continuous, non-intrusive data collection of an organization's cybersecurity performance — the ability of the measured organization to remediate cybersecurity findings quickly and effectively and on an ongoing basis.

By synthesizing complex cybersecurity risk into quantitative ratings and analytics, BitSight provides the marketplace with critical, timely and comparable insight into organizational cyber performance, helping to address historic information asymmetry challenges and self-disclosure biases without increasing the vulnerability of the rated entity. Thousands of investors, enterprises, insurers, government institutions and other market stakeholders trust BitSight's independent ratings and data to make better risk management decisions. Because of its global, Internet-wide scale, BitSight ratings currently cover all publicly traded U.S. companies.

Based on its extensive experience in the industry, BitSight believes that the new disclosure requirements envisioned by the Commission will allow both investors and companies to benefit from more standardized, timely, consistent and informative disclosure about cybersecurity risks and incidents. ***We urge the Commission to move forward with these requirements for the benefit of investors and other market participants.*** Some comments follow on specific questions asked in the Commission's proposal.

In response to Questions #17 and #50 regarding cyber risk management, strategy and governance disclosure, ***we recommend expanding the proposed narrative disclosure requirements to include quantitative, objective, risk-based metrics and measurements of a registrant's cybersecurity program*.** Our experience is that investors value quantitative, objective metrics and measurements regarding cybersecurity performance and outcomes.

Security performance metrics help investors assess the effectiveness of the policies, controls, governance and procedures that a company is implementing, providing investors greater visibility into how well the cyber risk program is being executed. Security performance measurements also provide investors with further validation of management's intentions.

[2] See Exhibit 2 of the Moody's Sector In-Depth Report, "SEC disclosure rules would improve transparency of cyber risk management," April 28, 2022. Research available at: https://www.moodys.com/researchdocumentcontentpage.aspx?docid=PBC_1323591

There are numerous examples of companies today disclosing relevant, detailed information on cybersecurity program performance for specific incidents as well as general risk disclosure, and directly benefiting from this transparency in the marketplace; illustratively:

- In 2019, Norsk Hydro was the victim of a ransomware attack that impacted operations. The company's response to the incident — which included a press conference featuring corporate executives, frequent, data-rich updates on the corporate blog, an engaged and knowledgeable leadership team, and sound financial estimates in quarterly filings — was widely praised by the market for providing timely, relevant information.[3]

  Notably, Norsk Hydro shared information about its cybersecurity program (including information about network segmentation, backup systems, and operational status), insurance coverage and the estimated total financial impact of the cyber attack in quarterly filings following the incident.[4]

- Following its severe breach in 2017, Equifax Inc. made significant investments in its cybersecurity program and began reporting on its changes. Beginning in 2020 and again in 2021, Equifax published the *Equifax Security Annual Report*, a public document that includes key security metrics and performance indicators that describe the state of the Equifax cybersecurity program.[5]

  Beyond describing the initiatives undertaken by the organization, the *Equifax Security Annual Report* details metrics and key results in key areas such as cloud security and supply chain assessments, security maturity benchmarking, and security performance benchmarking. These types of quantitative security indicators provide valuable validation for stakeholders that the Equifax security program is performing effectively, without creating new vulnerability to the company.

BitSight believes that all organizations should be similarly transparent about their cybersecurity program performance and results. Disclosure of risk-based performance metrics — including cybersecurity ratings created by independent, objective third parties — will provide investors access to appropriate and expanded information to make more informed decisions.

As to Questions #1 and #2, BitSight supports the overall aim of bolstering cybersecurity incident reporting. We would further suggest requiring companies to provide specific information about

---

[3] See "Experts praise Norsk Hydro cyberattack response," March 20, 2019, available at: https://www.techtarget.com/searchsecurity/news/252459949/Experts-praise-Norsk-Hydro-cyberattack-response

[4] See Norsk Hydro Q3 2019 press release, available at: https://www.hydro.com/en-DE/media/news/2019/third-quarter-2019-ramping-up-production-in-brazil-declining-market-prices/

[5] *Equifax Security Annual Report*, 2020 available at: https://assets.equifax.com/newsroom/2020-security-annual-report.pdf
Equifax Security Annual Report, 2021 available at: https://assets.equifax.com/marketing/US/assets/2021-security-annual-report.pdf

the nature of the incident to better inform investors and improve research efforts, which may in turn help prevent future incidents. Specifically, BitSight recommends:

- ***Disclosure of an incident should include whether the incident was originally detected by the company (or a contracted service provider) or by a third party, for example, law enforcement, government agencies, customers, journalists, or security researchers*.** Including this information will help partition incident disclosures into two broad categories: (a) self-detected, and (b) externally detected. Understanding how the incident was detected will help investors, regulators, and other interested parties comparatively determine the effectiveness of the company's security policies, program, and controls.

As to Questions #17 and #20, we believe adding more specific risk disclosures covering key cybersecurity practices would help investors, credit analysts, regulators, and customers gain a deeper understanding of individual company cybersecurity posture and offer a mechanism for comparing companies that are regulated by the Commission. As examples, we encourage the Commission to consider the following, particularly with respect to Proposed Item 106(b):

- ***Disclosure regarding the last time that specific independent security assessments and testing were conducted by the company*.** Granularity of this requirement would need to be considered but could include requiring disclosure of whether an application penetration test, red team exercise, or security control program assessment was performed in the previous calendar year. The resulting disclosure will help investors determine whether or not the company is seeking outside help in assessing its security defenses on a periodic basis.

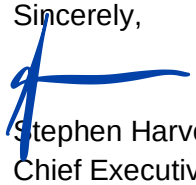
- ***Disclosure about the reporting line of the Chief Information Security Officer (CISO) or equivalent individual in the organization*** would help investors and other interested parties determine whether the CISO has enough visibility at senior leadership levels.

- ***Disclosure of whether the CISO participates in some form of executive session on at least an annual basis with one or more board members, such as the chair of the Risk or Audit Committee*,** would further illuminate which companies are considering the independence of the CISO and associated security decision making.

Finally, with respect to Questions #5 and #8, we believe it would be prudent for the Commission to further ***clarify its definition of materiality for purposes of reporting cybersecurity incidents*** in order to avoid wide latitude for interpretation and corresponding uneven thresholds for disclosure. By providing updated guidance, the Commission can reduce the likelihood that events which should otherwise be reported remain undisclosed. We also believe the Commission should consider whether financial benchmarks, e.g., percentage of revenue, can be used to help determine materiality, and that it would be worthwhile to engage industry experts among the cybersecurity and financial community for further input.

In conclusion, we applaud the Commission's approach and appreciate the opportunity to comment on this critical initiative to improve investor understanding and market transparency for corporate cyber risk and incidents. We at BitSight stand ready to support your efforts.

Sincerely,



Stephen Harvey
Chief Executive Officer
BitSight Technologies, Inc.