NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC.
750 First Street N.E., Suite 1140
Washington, D.C. 20002
202-737-0900
Fax: 202-783-3571
www.nasaa.org

June 18, 2019

The Honorable Jack Reed
Unites States Senator
728 Hart Senate Office Building
Washington, DC 20510

Re: Cybersecurity Disclosure Act of 2019 (S. 592)

Dear Senator Reed:

On behalf of the North American Securities Administrators Association (NASAA),[1] I am writing to express support for S. 592, the "Cybersecurity Disclosure Act of 2019," which would require that publicly traded companies disclose in annual filings with the U.S. Securities and Exchange Commission ("SEC") whether any member of their governing body, such as their board of directors or general partner, possesses expertise or experience in cybersecurity. If no member has such expertise or experience, such companies would be required to detail what-if-any other cybersecurity considerations were taken into account by the persons responsible for identifying and evaluating nominees for the governing body.

Incentivizing publicly traded companies to consider whether or not they have appropriate cybersecurity expertise on their governing body is a common-sense way to promote greater attention to cybersecurity risk by public corporations. Investors and customers are well-served by policies that encourage companies to consider such risks proactively, as opposed to after a data breach has already occurred, when such investors and customers have already been harmed. Importantly, S. 592 would not require companies to do anything beyond disclosing information; the bill merely nudges companies to act in their own best interests by creating an incentive for them to treat cybersecurity expertise as a priority at the senior leadership level. This is good news for companies and investors.

Cyberattacks on U.S. companies and businesses continue to increase in both frequency and sophistication. Investors are at significant risk considering that the number of exposed records containing personally identifiable information increased by 126% between 2017 and 2018, according to the Identity Theft Resource Center.[2] NASAA Past-President Joseph Borg previously authored an op-ed highlighting the growing concern over the number of cyberattacks perpetrated against

[1] The oldest international organization devoted to investor protection, NASAA was organized in 1919. Its membership consists of the 67 state, provincial, and territorial securities regulatory agencies of the United States, Canada, and Mexico. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

[2] Identify Theft Resource Center. "2018 End-of-Year Data." Jan. 28, 2019. Available at https://www.idtheftcenter.org/2018-end-of-year-data-breach-report.

companies and the efforts state securities regulators are taking to assist small and mid-sized investment advisers to improve their cybersecurity practices.[3]

Thank you for your consideration of NASAA's views. If we may be of further assistance, please do not hesitate to contact me or Michael Canning, NASAA's Director of Policy and Government Affairs, at (202) 737-0900.

Sincerely,

Michael S. Pieciak
NASAA President,
Commissioner, Vermont Department of Financial Regulation

[3] Borg, Joseph P. "Everyone has a Role in Protecting against Cyberattacks". September 5, 2017. Available at www.americanbar.org/content/dam/aba/administrative/business_law/newsletters/CL680000/full-issue-201709.authcheckdam.pdf