

United States Senate

WASHINGTON, DC 20510

February 8, 2022

The Honorable Gary Gensler
Chair
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chair Gensler:

We write to urge the Securities and Exchange Commission to propose rules regarding cybersecurity disclosures and reporting. We further urge you to coordinate the formulation of these rules with the National Cyber Director.

As you know, cybersecurity is among our most significant national security and economic challenges. Daily interactions increasingly take place in cyberspace, leading to more persistent and complex cybersecurity threats. Costs of cyber attacks have also been on the rise. Investors often bear these costs because a serious cyber attack can permanently affect a company's valuation and profitability.

During your most recent testimony before the Senate Banking Committee, you stated that you have asked the SEC staff to develop proposals on cybersecurity disclosures and incident reporting. You reiterated in public remarks last month that companies and investors would benefit if information on cybersecurity risk "were presented in a consistent, comparable, and decision-useful manner."

We applaud your efforts to promote transparency and oversight of cybersecurity risks at public companies and at financial sector registrants like investment funds, investment advisers, and broker-dealers. Investors deserve a clear understanding of whether companies and investment managers are prioritizing cybersecurity. They also have a right to prompt notification of serious cybersecurity incidents. More information will enable investors to hold companies and investment managers accountable.

One effective regulatory approach would be asking public companies to disclose whether a cybersecurity expert is on the board of directors, and if not, why not. We have sponsored bipartisan legislation called the Cybersecurity Disclosure Act to require companies to provide this disclosure to investors. The bill does not tell companies how to deal with cybersecurity threats. How a company chooses to address cybersecurity risks would remain its own decision. Boards of directors would be encouraged to develop approaches that address their own needs. The goal is to encourage directors to play a more effective role in cybersecurity risk oversight.

Public companies and investment managers should pay attention to threats before they are realized. This is a better approach than scrambling to figure out what went wrong after investors have been harmed. America's economic prosperity is linked to strong cybersecurity defenses in the private sector. The alternative unfortunately puts investors' hard-earned savings and pensions at risk. We are encouraged that the SEC intends to address cybersecurity threats using a wide variety of tools, from raising the bar on risk management to clarifying when to report a serious breach that has already occurred.

Thank you for your attention to this important matter. Please keep our staffs informed of the SEC's progress on improving cybersecurity disclosures and reporting by public companies and financial sector registrants.

Sincerely,



Jack Reed
United States Senator



Mark R. Warner
United States Senator



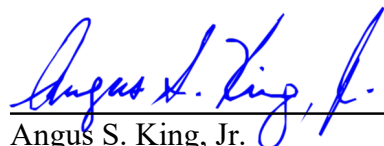
Catherine Cortez Masto
United States Senator



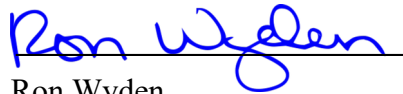
Kevin Cramer
United States Senator



Susan M. Collins
United States Senator



Angus S. King, Jr.
United States Senator

A handwritten signature in blue ink that reads "Ron Wyden". The signature is written in a cursive style and is positioned above a horizontal line.

Ron Wyden
United States Senator

cc: John Christopher Inglis, National Cyber Director