

United States Senate

WASHINGTON, DC 20510

May 11, 2011

Ms. Mary Schapiro
Chairman
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549

Dear Chairman Schapiro,

Securing cyberspace is one of the most important and urgent challenges of our time. Every day, malicious actors attack and disrupt computer networks to steal valuable trade secrets, intellectual property, and financial and confidential information, causing significant damage to the United States government, our citizens, our businesses, and our economy. In light of the growing threat and the national security and economic ramifications of successful attacks against American businesses, it is essential that corporate leaders know their responsibility for managing and disclosing information security risk. Given inconsistencies in reporting, investor confusion, and the national importance of addressing cyberspace security, we request that the Securities and Exchange Commission issue guidance regarding the disclosure of information security risk, including material network breaches.

While the benefits of information technology – increased productivity, reduced costs, and new efficiencies in communication – are obvious, the risks are not well known or understood. Difficulties in measuring the value of information stored within a computer network, evaluating the effectiveness of security controls, defending against capable and determined attackers, and assessing and quantifying the consequences of a breach are only some of the myriad challenges that corporate leaders face in evaluating their information security risk. Though managing information security risk is not an exact science, it is a core responsibility shared by leaders and managers throughout all levels of a business.

The Commission promotes corporate accountability for risk management through the enforcement of material risk disclosure. If properly assessed, disclosed information allows investors to consider and value a company's material risks – including material information security risks – in investment decisions, spurring companies to understand and reduce their risk exposure to attract further capital. Unfortunately, a substantial number of companies do not report their information security risk to investors. For instance, a 2009 survey conducted by Hiscox, an insurance underwriter, found that 38 percent of Fortune 500 companies made a “significant oversight” by not mentioning privacy or data security exposures in their public

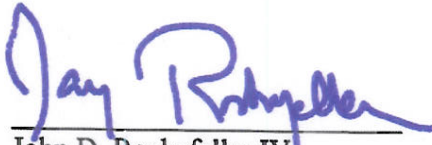
filings. In addition to reporting inconsistencies, it is unclear whether corporations who do disclose their information security risk exposure are adequately assessing and mitigating these risks. In our review of recent disclosures, we found statements ranging from boilerplate descriptions of risk to details of specific attacks; we did not, however, find information on steps taken by the corporation to reduce risk exposure.

Beyond our concerns about material information security risk, we believe that once a material network breach has occurred, leaders of publicly traded companies may not fully understand their affirmative obligation to disclose information on potentially compromised intellectual property or trade secrets. Federal securities law obligates the disclosure of any material network breach, including breaches involving sensitive corporate information that could be used by an adversary to gain competitive advantage in the marketplace, affect corporate earnings, and potentially reduce market share. Again, our review of recent corporate disclosures suggests that material breach reporting, like information risk, is inconsistent and unreliable. We are concerned that the lack of quality, public information in these matters enables an inefficient marketplace that devalues security and impairs investor decision-making.

The Commission, with its authority to protect investors and promote fair and efficient markets, has previously provided public companies with interpretive guidance on existing disclosure requirements. We request that the Commission develop and publish interpretive guidance clarifying existing disclosure requirements pertaining to information security risk, including material information security breaches involving intellectual property or trade secrets. In undertaking this effort, we also ask that the Commission examine how important market participants – such as credit rating agencies and securities analysts – incorporate evidence of information security risk into their assessments of companies and investment products. We believe this guidance, undertaken using longstanding Commission legal authority, will enhance investor and corporate awareness of information security risk, thus improving the national and economic security of our nation.

Thank you for your assistance in this critical effort. We ask that you please provide a response regarding your plans to consider our request.

Sincerely,



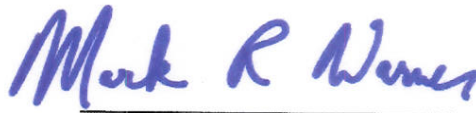
John D. Rockefeller IV
Chairman
Commerce, Science, and
Transportation Committee



Robert Menendez
United States Senator



Sheldon Whitehouse
United States Senator



Mark Warner
United States Senator



Richard Blumenthal
United States Senator