JAMES R. LANGEVIN
2D DISTRICT, RHODE ISLAND

COMMITTEE ON ARMED SERVICES
EMERGING THREATS AND CAPABILITIES (RANKING)
SEAPOWER AND PROJECTION FORCES

COMMITTEE ON HOMELAND SECURITY
CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES
COUNTERTERRORISM AND INTELLIGENCE

ES153466

Congress of the United States
House of Representatives
Washington, DC 20515–3902

WASHINGTON OFFICE
109 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225-2735
FAX: (202) 225-5976

DISTRICT OFFICE:
THE SUMMIT SOUTH
300 CENTERVILLE ROAD, SUITE 200
WARWICK, RI 02886
TELEPHONE: (401) 732-9400
FAX: (401) 737-2982

http://langevin.house.gov

June 17, 2015

The Honorable Mary Jo White
Chair
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: Disclosure Effectiveness Review

Dear Chair White:

We are writing regarding the need to update the SEC's cybersecurity disclosure guidance for publicly traded companies. We understand that the Division of Corporate Finance is undertaking a review of the disclosure process to increase transparency and information. Cyber and cybersecurity disclosures are a clear and discrete area where investors need more relevant and timely information.

Institutional investors, private investors, and public pension funds should be able to compare the robustness of cybersecurity protections and controls between companies within the same sector. As outlined in the March Harvard Business Review article *Why Data Breaches Don't Hurt Stock Prices*, shareholders still don't have good metrics, tools, and approaches to measure the medium- and long-term impact of cyber attacks on businesses, and, as a result, are unable to make an accurate assessment of share value. Every company regulated by the SEC is in some way a digital company, and thus subject to risks that include loss of intellectual property, disclosure of sensitive data, and loss of customer confidence. While difficult to measure, all of these threats can result in a loss of market share.

To better understand the SEC's approach to these persistent challenges, we request you describe:

1. How cybersecurity fits into the SEC's disclosure review process.
2. Your views on how updating cybersecurity disclosure would enhance investor protection.
3. Who should be responsible for a registrant's cybersecurity practices.
4. Who is responsible for determining a registrant's best practices and how they are maintained.
5. How the SEC currently evaluates registrant determination of cyber practice effectiveness.

PRINTED ON RECYCLED PAPER

6. What events or circumstances will require an 8-K filing with respect to a cyber attack or breach.
7. Whether any recent facts or circumstances have called into question existing SEC disclosure guidance regarding cybersecurity practices.
8. Whether any recent facts or circumstances have called into question the SEC's internal cybersecurity practices.

Cyber attacks and cyber risk can pose a systemic threat to the marketplace, not just to an individual firm or its customers. Estimates of the economic costs of commercial cyber-espionage to the United States top $100 billion annually. Such costs are rarely, if ever, reflected in financial statements.

We urge the Commission to consider directing issuers to disclose in 10-K reports a clear description of:

1. How the registrant determines the best cybersecurity practices for its industry;
2. The registrant's present state of conformity to those practices;
3. The registrant's plan and schedule for achieving full conformity;
4. How the registrant is ensuring that its best practices are improved and updated in response to evolving threats; and,
5. The frequency with which the registrant's CEO, CFO, and Board of Directors are briefed on cyber/information security incidents.

These recommendations are consistent with those included in the President's Council of Advisors on Science and Technology (PCAST) November 2013 report *Immediate Opportunities for Strengthening the Nation's Cybersecurity* and will not increase corporate vulnerability or provide a roadmap for illicit actors to compromise systems. The answers to these questions would provide important information to investors and the public about the risks companies face and how companies are working to mitigate those risks.

SEC regulation and guidance must be updated to better align with the very real threats we face. As stated in the PCAST report, "because cyber risks can cascade, and are correlated across the whole economy, traditional standards of materiality may be naïve." Adjusting disclosures as we suggest will help ensure that investors have necessary information while also giving the SEC essential data to protect the markets as a whole. As we are sure you are aware, on May 19, 2014, the Department of Justice charged members of the Chinese military with conducting economic cyber-espionage against American companies, including Alcoa, Allegheny Technologies Incorporated, and U.S. Steel. As outlined by the DoJ, the alleged hacking was conducted solely to advantage state-owned companies and other interests in China at the expense of businesses here in the United States.

This type of disclosure will also enhance the SEC's stated goals of reduced repetition in disclosure documents. As your staff is well aware, disclosures, particularly those concerning cybersecurity (when provided at all), often repeat language verbatim year after year, despite the

fact that the cyber threat environment and awareness of vulnerabilities are constantly evolving. Companies often fail to include any meaningful cyber information until after a breach and then often fail to amend or update that language in subsequent years. This information is not useful for investors; moreover, the lack of information on cybersecurity may place retail investors at a disadvantage as they do not have the resources to investigate whether companies in similar asset classes have dramatically different exposures on account of their cyber controls and practices. This is not entirely the fault of companies: materiality as it relates to cyber risk is particularly difficult to assess both because we lack sufficient data from past cyber attacks and because the effects are often not distinguishable from the many confounding variables surrounding a company's earnings.

What gets measured gets managed. Companies must invest in practices and protocols to continuously identify and mitigate their exposure to cyber risk by fully understanding their own vulnerabilities and the threat actors. Protecting intellectual property, trade secrets, and customer information must be a priority for government, corporations and consumers alike – it should be viewed not as a cost, but as an investment. A robust, secure supply chain, be it for physical goods or the transmission and storage of information, is critical for businesses and is in the interest of all parties.

As the SEC continues to undertake a review of disclosures, we urge you to take action on cybersecurity disclosure and also to expand your understanding of the current state of cybersecurity. In keeping with the evolving nature of technology and of the cyber threat, we encourage the SEC to build a robust reevaluation process into future guidance in order to ensure that investors are provided the most relevant information. We hope you will focus on processes rather than specific controls, so that both your regulators and investors are able to develop an understanding of a company's cybersecurity posture and the target profile of the level of security they are trying to achieve.

We appreciate your attention to this matter and look forward to hearing more about the steps the SEC is taking on cybersecurity.

Sincerely,

Jim Langevin
Member of Congress

Jim Himes
Member of Congress