Langevin, Himes Urge SEC to Update Cybersecurity Disclosures

JUN 18, 2015 | ISSUES: CYBERSECURITY

Congressmen Jim Langevin (D-RI) and Jim Himes (D-CT) sent a letter today to Securities and Exchange Commission (SEC) Chair Mary Jo White, underscoring the need to update the SEC's cybersecurity disclosure guidance for publicly traded companies. The letter comes as the Division of Corporate Finance is undertaking a review of the disclosure process.

"The costs of cyber espionage are substantial, resulting in the loss of intellectual property, economic competitiveness and consumer confidence – not to mention the significant financial impact – and yet companies often fail to disclose the cybersecurity strategy they use to evaluate these threats," said Langevin, co-chair of the bipartisan Congressional Cybersecurity Caucus and a senior member of the House Committee on Homeland Security, who serves on Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies. "Investors deserve to know what preventative measures are being taken against cyber risks, and consumers deserve to know how their private information is being protected. SEC guidance must reflect the current threat landscape and the evolving technology challenges that companies face."

"Every year we see more and more cyber attacks on companies, and the attackers are growing bolder and more sophisticated," said Himes, who serves on the Financial Services Committee and the House Permanent Select Committee on Intelligence. "These cyber threats can have a chilling effect on investors and consumers unless they know that the proper efforts are being taken to secure private information properly. We look to the SEC to lead in this situation and set industry-wide standards for all listed companies."

Among other recommendations in the letter, Langevin and Himes are urging the SEC to consider directing each company to disclose in 10-K reports a clear description of how it determines the best cybersecurity practices for its industry. Combined with disclosures of the company's present state of conformity to those practices; its plan and schedule for achieving full conformity; and how it is ensuring that its best practices are improved and updated in response to evolving threats, investors and consumers would have a common

framework in which to compare businesses. Langevin and Himes also encourage the SEC to require companies to disclose the frequency with which their CEO, CFO and Board of Directors are briefed on cyber and 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.

In addition to providing guidance for companies, Langevin and Himes are asking the SEC to outline how cybersecurity fits into their disclosure review process and encouraging the SEC to build a robust reevaluation process into future guidance. They also request that the SEC describe what circumstances would require an 8-K filing with respect to a cyberattack or breach. The letter encourages the SEC to focus on processes rather than specific controls, so regulators and investors are able to develop an understanding of a company's cybersecurity posture and their target security profile.

Document

- Letter to SEC Chairwoman Mary Jo White.