

Securities Law and Legislative ADVISORY

October 20, 2011

SEC's Division of Corporation Finance Issues Interpretive Guidance Related to Cybersecurity Disclosures

On October 13, 2011, the Staff of the Security and Exchange Commission's (SEC) Division of Corporation Finance issued guidance¹ (the "Cybersecurity Guidance" or "Guidance") regarding its views on disclosure obligations relating to cybersecurity risks and cyber incidents. The Staff took this action in response to various political pressures, including a letter dated May 11, 2011, from Senator Jay Rockefeller (D-WV) and four other senators to SEC Chairman Mary Schapiro.²

The Cybersecurity Guidance makes clear that the statements contained therein represent only the views of the Staff, and that "the Commission has neither approved nor disapproved its content." Nonetheless, the Guidance provides important insight into the direction the SEC may be going in requiring registrants to disclose information about their cybersecurity practices.

The issuance of the Guidance is also likely to be used by the White House, Congress and other federal policy makers to promote the need for more extensive federal cybersecurity statutes and regulations that would impose affirmative obligations on businesses to better protect their cyber networks and make public disclosures (beyond SEC filings) about security breach incidents. On May 12, 2011, the Obama Administration released its cybersecurity legislative proposal,³ as required in the Cyberspace Policy Review⁴ and in response to a request from Senate Majority Leader Harry Reid (D-Nev.) and six other Senate committee chairs for draft cybersecurity legislation. Additionally, on October 5, 2011, the House Republican Cybersecurity Task Force issued a report with its recommendations on federal cybersecurity legislation pursuant to a request by the House Republican leadership.⁵ The Task Force's report examined four critical

¹ Division of Corporate Finance, Securities and Exchange Commission, *CF Disclosure Guidance: Topic No. 2: Cybersecurity* (Oct. 13, 2011), available at <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

² Letter from Senator John D. Rockefeller, IV to Mary Schapiro, Chairman of the United States Securities and Exchange Commission (May 11, 2011), available at http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e.

³ The White House, *Fact Sheet: Cybersecurity Legislative Proposal* (May 12, 2011), available at: <http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>. See also Alston & Bird Privacy + Security Blog, *White House Releases Cybersecurity Plan* (May 25, 2011), available at: <http://www.alstonprivacy.com/blog.aspx?entry=4325>.

⁴ The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 29, 2009), available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. See also The White House, *Fact Sheet: Cyberspace Policy Review* (May 29, 2009), available at: <http://www.whitehouse.gov/the-press-office/cybersecurity-event-fact-sheet-and-expected-attendees>.

⁵ *Recommendations of the House Republican Cybersecurity Task Force* (October 5, 2011), available at: http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf. See also Alston & Bird Privacy + Security Blog, *House Republican Cybersecurity Task Force Releases Recommendations* (October 5, 2011), available at: <http://www.alstonprivacy.com/blog.aspx?entry=4412>.

areas: critical infrastructure and incentives, information sharing and public-private partnerships, existing cybersecurity laws and legal authorities. Given this political backdrop, the Guidance could be viewed as the first step in a broad federal government initiative to raise the standards of cybersecurity practices across the industry.

What Disclosures Does the Cybersecurity Guidance Recommend?

The Guidance presents the Staff's advice on how registrants, including all public companies, should consider and disclose possible cybersecurity issues under existing SEC rules. The Guidance includes sections on how registrants should disclose cybersecurity issues in various sections of their public reports, including Risk Factors, Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A), Description of Business, Legal Proceedings and financial statement disclosures. While not a formal interpretation, the Guidance provides valuable insight into the sort of disclosure practices registrants should consider when evaluating their own cybersecurity (including risks and incidents).

In particular, the Guidance clarifies registrants' responsibility to discuss cybersecurity and cyber incidents in the risk factors and MD&A sections of their public reports. In describing risk factor disclosure obligations related to cybersecurity, the Guidance notes that registrants should make disclosure if "these issues are among the most significant factors that make an investment in the company speculative or risky." This type of analysis should include all relevant information, including current cybersecurity practices and past cyber incidents. Additionally, consistent with Regulation S-K Item 503(c), the risk disclosure should describe the nature of the material risk and how that risk might affect the registrant. Examples of appropriate disclosures might include:

- aspects of the registrant's business that gave rise to material cybersecurity risks and the possible costs;
- descriptions of cyber incidents that are individually or in the aggregate material; and
- risks related to cyber incidents that could remain undetected for an extended period.

The Guidance also notes that discussion of cybersecurity issues may be required in MD&A if one or more known cyber incidents, or if the risks of any potential incident, are likely to materially affect the registrant's results of operations, liquidity or financial condition. Disclosure may also be required if such an incident would cause reported financial information to be not necessarily indicative of future operating results or financial condition. For instance, disclosure would be required if material intellectual property were stolen during a cyber-attack and the effects of the theft were reasonably likely to be material.

Are These New Disclosure Requirements?

No, these are not new SEC disclosure requirements. However, from time to time, the SEC Staff will issue disclosure guidance in order to focus registrants' attention on existing disclosure requirements that the Staff wants registrants to focus on. The SEC has issued similar guidance in the past on a variety of topics, including political risks in foreign operations, Y2K and the effects of climate change.⁶

In this instance, the Guidance clarifies what the Staff believes the current SEC rules require with respect to cybersecurity and cyber incidents. For instance, the Guidance points out that while no existing disclosure requirements refer specifically to cybersecurity risks and cyber incidents, a number of current disclosure requirements may include an

⁶ For our previous Securities Law Advisory on Climate Change, see Alston & Bird LLP, *SEC Issues Interpretive Guidance Related to Climate Change Disclosure and Proposes Changes to Rule 10b-18* (Jan. 28, 2010), available at http://www.alston.com/securities_climate.

obligation to disclose such risks and incidents. As with any type of information, registrants are required to disclose material information about cybersecurity risks and incidents when necessary to make other required disclosures not misleading.

What Should Companies Do Now?

In general, registrants should bear in mind that cybersecurity practices and cyber incidents should be disclosed in their public reports if those practices and incidents are material. In particular, registrants may want to:

- review, and possibly revise disclosure controls and procedures in order to capture cybersecurity-related issues;
- educate members of the disclosure committee or other members of management responsible for disclosure about cybersecurity issues;
- undertake a specific review of any existing internal assessments of the possible impact of cybersecurity practices and cyber incidents on the company's operations or prospects;
- revisit existing disclosures regarding the company's business, including MD&A and risk factors, to determine whether additional or revised disclosures are necessary; and
- assess the risk and consider whether to engage policy makers regarding additional cybersecurity legislative and regulatory proposals currently being considered in Washington that may also impact a registrant's cybersecurity practices.

*This advisory was written by **Dave Brown, Charlie Yates and Paul Martino.***

For more information, contact your Alston & Bird LLP attorney or one of the attorneys in the firm's [Securities Group](#), [Legislative Group](#) or [Privacy & Security Task Force](#).

For other related securities advisories, [click here](#). If you or a colleague would like to receive future *Securities Law Advisories* and *Special Alerts* electronically, please forward your contact information, including your e-mail address, to securities.advisory@alston.com. Be sure to put "subscribe" in the subject line.