SUTHERLAND

LEGAL ALERT

October 26, 2011

Who Is Listening? The SEC Emphasizes Importance of Cybersecurity Disclosure

The U.S. Securities and Exchange Commission (SEC) staff recently issued guidance concerning its views on disclosure obligations related to cybersecurity risks and cyber incidents.[1] The SEC staff issued the guidance in response to a letter that SEC Chairman Mary Schapiro received in May 2011 from five U.S. Senators requesting that the SEC publish interpretive advice "clarifying the existing disclosure requirements pertaining to information security risk, including material information security breaches involving intellectual property or trade secrets."[2]

This guidance may be followed by additional legislative and regulatory action in light of the attention cybersecurity has received over the last several years.[3] Some of these legislative or regulatory actions may even have an impact on the SEC disclosure obligations of public companies. For example, the Obama Administration presented draft legislation relating to cybersecurity to the Congress that would, among other things, require the chief executive and other executive officers of public companies to include a certification in their public SEC reports regarding their development and implementation of a cybersecurity plan for their companies and the effectiveness of the plan in mitigating identified cybersecurity risks.[4]

Overview of the Guidance

The SEC staff guidance clarifies that even though the SEC's existing disclosure rules do not specifically reference cybersecurity, public companies should consider the growing importance of cybersecurity and make appropriate disclosures "consistent with the relevant disclosure considerations that arise in connection with any business risk." In this regard, the guidance is similar to guidance that the SEC has issued in the past relating to foreign political risks and climate change.[5]

In particular, the guidance addresses disclosure considerations pertaining to cybersecurity and cyber incidents in the following areas:[6]

- **Risk Factors.** Companies should discuss cybersecurity risks in their risk factors if "these issues are among the most significant factors that make an investment in the company speculative or risky." Relevant considerations include current cybersecurity practices and past cyber incidents, and how future incidents or breaches might increase costs, affect customer bases, or infringe on

[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 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] For example, Sony Corporation was subject to cyber attacks in Spring 2011 resulting in the loss of sensitive information of users of its PlayStation®Network, and the computer systems of Radisson Hotels were hacked in 2008 and 2009 resulting in the loss of customer credit and debit card information.
[4] *Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act* (May 2011), available at http://democrats.senate.gov/pdfs/WH-cyber-critical-infrastructure-provisions.pdf.
[5] For more on the climate change guidance, see Sutherland Legal Alert: "SEC Warms to Climate Change," March 16, 2010.
[6] The guidance notes that companies should avoid disclosing a level of detail that would compromise cybersecurity.

proprietary information. As with all risk factors, companies should focus on specific cyber risks and avoid boilerplate risk language.

- **MD&A.** A cyber incident or cybersecurity risk should be discussed in MD&A if it is likely to materially affect a company's results of operations, liquidity or financial condition.

- **Description of Business.** A cyber incident should be mentioned in Description of Business if it materially affects a company's products or services, relationships with customers and suppliers, or competitive conditions.

- **Legal Proceedings.** A company may need to disclose a cyber incident if it gives rise to a material legal proceeding, such as a class action suit for loss of sensitive customer information.

- **Financial Statement Disclosures.** Companies should be mindful of the accounting-related implications of cyber incidents and ensure that they are accounted for appropriately in their financial statements. For example, after a cyber incident, companies may offer customers additional incentives to encourage customer loyalty and incur significant losses and reduced cash flows resulting in impairment of certain assets.

- **Disclosure Controls and Procedures.** If a cyber incident could negatively affect a company's ability to process and report information to the SEC, management should consider whether the company's disclosure controls and procedures are ineffective.

Next Steps

In light of the guidance, companies should consider taking the following steps:

- Review existing cybersecurity practices and the impact of past cyber incidents on the company's operations.

- Assess the sufficiency of current cyber disclosure and compare such disclosure to that of industry peers.

- Analyze disclosure controls and procedures to ensure they adequately account for cybersecurity issues, and apprise members of the disclosure committee or management in charge of SEC reporting matters of the recent guidance.

- In the case of companies subject to Regulation S-P's information security requirements, including investment companies, carefully review written policies and procedures to ensure they are up-to-date and consistent with their disclosure.

- Evaluate the impact of other legislative and regulatory proposals relating to cybersecurity to determine what actions are needed, including taking steps to influence the final form of new legislation or rules.[7]

[7] See, e.g., *Recommendations of the House Republican Cybersecurity Task Force* (October 5, 2011), available at http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf; 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.

■ ■ ■

If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed below or the Sutherland attorney with whom you regularly work.

Cynthia M. Krus	202.383.0218	cynthia.krus@sutherland.com
John J. Mahon	202.383.0515	john.mahon@sutherland.com
Harry S. Pangas	202.383.0805	harry.pangas@sutherland.com
John H. Walsh	202.383.0818	john.walsh@sutherland.com
Stephani M. Hildebrandt	202.383.0845	stephani.hildebrandt@sutherland.com
Vlad M. Bulkin	202.383.0815	vlad.bulkin@sutherland.com
Terri Ginsberg	202.383.0976	terri.ginsberg@sutherland.com
Lisa A. Morgan	202.383.0523	lisa.morgan@sutherland.com
Owen J. Pinkerton	202.383.0254	owen.pinkerton@sutherland.com
Darius I. Ravangard	202.383.0891	darius.ravangard@sutherland.com
Bradford J. Sayler	202.383.0837	brad.sayler@sutherland.com
Payam Siadatpour	202.383.0278	payam.siadatpour@sutherland.com