Morgan Lewis

energy lawflash alert

www.morganlewis.com

SEC Issues Guidance on the Disclosure of Cybersecurity Incidents and Costs

October 19, 2011

On October 13, the U.S. Securities and Exchange Commission (SEC) issued disclosure guidance[1] related to cybersecurity risks and costs that may have far-reaching impacts on electric utilities. For those electric utilities already subject to the North American Electric Reliability Corporation (NERC) cybersecurity requirements, this guidance suggests the need for increased scrutiny of compliance costs and harms resulting from cyber incidents and potential cyber incidents to evaluate appropriate disclosure. With the pending increase in the number of assets covered by the Version 4 Critical Infrastructure Protection (CIP) Reliability Standards, which the Federal Energy Regulatory Commission (FERC) recently proposed to approve, the costs of compliance are likely to significantly increase across the electric utilities industry, affecting a wide variety of SEC registrants subject to FERC's reliability jurisdiction.

The SEC's guidance was spurred by its recognition that registrants have been relying more heavily on digital technologies for their operations, which results in increased risks to those operations due to cyber vulnerabilities. The SEC explained that cyber incidents, including cyber attacks and unintentional cyber events, can lead a registrant to incur substantial costs and suffer negative consequences including the following:

- Remediation costs, such as for asset repairs, customer incentives, and liability for lost assets
- Increased costs for cybersecurity protective measures
- Lost revenues from the proprietary information obtained by others or the loss of customers
- Litigation
- Reputational damage

The SEC explained that, while no disclosure requirements mention cyber events and cyber risks, certain disclosures may nevertheless be required because cyber risks and cyber incidents would be captured by existing disclosure requirements that deal with operational and financial risks. The SEC suggested that registrants use their new guidance to "review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents."

1. View the guidance online at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Risk Factors

First, registrants are expected to disclose cyber incident risks if such risks are among the factors that make a particular investment risky or speculative. Such disclosures should include the nature of the material risks and the impact of each risk on the registrant. The SEC offered the following as examples of appropriate disclosures:

- Business characteristics that create material cybersecurity risks, with potential costs and consequences
- Outsourcing that creates cybersecurity risks, and how those risks are addressed
- Cyber incidents experienced by the registrant, with costs and consequences of those incidents
- Risks for cyber incidents that may remain undetected for a lengthy period of time
- Relevant insurance coverage

In addition, the SEC explained, past cyber incidents may need to be discussed to place the risk discussion in context, including a description of any specific attacks and the costs and consequences from such attacks.

Management's Discussion and Analysis (MD&A) of Financial Condition and Results of Operations

Second, the SEC explained that cybersecurity risks and cyber incidents should be addressed in a registrant's MD&A if the costs and consequences of the risks and incidents "represent a material event, trend, or uncertainty that is reasonably likely to have a material effect" on the operations or the financial condition of the registrant. If it is "reasonably likely" that reductions in revenue, cyber protection costs, litigation, or the like will occur, those outcomes should be discussed. Similarly, even if no harm occurred, but cyber protections were materially increased as a result of a cyber incident, those costs should be disclosed. Presumably, this disclosure would be necessary only if material.

Description of Business

Third, the SEC explained that cyber incidents that "materially affect" a registrant's products, services, client relationships, and the like should be disclosed in the "Description of Business." For example, a cyber incident that threatens the viability of a new product that a registrant is developing may need to be discussed.

Legal Proceedings

Fourth, the SEC explained that litigation resulting from a cyber incident may need to be disclosed if the litigation is material.

Financial Statement Disclosures

Fifth, the SEC discussed financial statement disclosures, and explained that cybersecurity risks and cyber incidents could affect financial statements in several ways. Prior to a cyber incident, substantial costs may be incurred to protect against cyber incidents. For electric utilities, this might include the costs for compliance with mandatory CIP Reliability Standards as well as other corporate cybersecurity measures.

During and after a cyber incident, registrants may try to mitigate damages to customer relationships by offering incentives, may need to recognize losses due to asserted and unasserted claims, or may suffer cash flow reductions that potentially impair assets such as goodwill, trademarks, patents, capitalized software, and intangible customer-related assets. In the event of a cyber incident, a registrant must try to determine the impact of the incident on its financial statements by reassessing estimates used in preparing such financial statements, including estimates relating to warranties, litigation, and deferred revenue.

Disclosure Controls and Procedures

Finally, conclusions reached by a registrant regarding the effects of a cybersecurity incident on its disclosure controls and procedures would need to be disclosed if the incident created a risk to the ability of the registrant to "record, process, summarize, and report" information disclosed in SEC filings.

If you have any questions concerning the information discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

Washington, D.C.

John D. McGrane	202.739.5621	jmcgrane@morganlewis.com
Stephen M. Spina	202.739.5958	sspina@morganlewis.com
J. Daniel Skees	202.739.5834	dskees@morganlewis.com

About Morgan, Lewis & Bockius LLP
With 22 offices in the United States, Europe, and Asia, Morgan Lewis provides comprehensive transactional, litigation, labor and employment, regulatory, and intellectual property legal services to clients of all sizes—from global Fortune 100 companies to just-conceived startups—across all major industries. Our international team of attorneys, patent agents, employee benefits advisors, regulatory scientists, and other specialists—nearly 3,000 professionals total—serves clients from locations in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.