SEC Cybersecurity Disclosure for Publicly Traded Companies, Including Government Contractors

In May 2011, prompted by recent high-profile data security breaches in the public and private sectors, several senators led by Senate Commerce Chairman Jay Rockefeller, IV (D-WV) requested that the Securities and Exchange Commission (SEC) develop and publish interpretive guidance clarifying existing disclosure requirements pertaining to information security risk.[1] In response to this letter, on October 13, 2011, the SEC's Division of Corporation Finance issued disclosure guidance on cybersecurity risks and cyber incidents as part of its CF Disclosure Guidance series (CF Guidelines).[2] The CF Guidelines do not reflect the views of the SEC and do not create any new disclosure obligations. Rather, the CF Guidelines reflect the Division of Corporation Finance staff's interpretation of how existing disclosure requirements apply to cybersecurity risks and cyber incidents.

Despite the nonbinding nature of the CF Guidelines, Senator Rockefeller expressed his satisfaction with them, writing, "[t]his guidance changes everything. It will allow the market to evaluate companies in part based on their ability to keep their networks secure."[3] In reality, the CF Guidelines likely foreshadow staff comments that will be issued on SEC filings. Eventually, reporting companies will also have to situate the SEC reporting guidance into the cybersecurity disclosure rules proposed by the Obama administration that are currently being debated in Congress which would create civil and criminal penalties for failure to report cybersecurity incidents.[4]

While applicable to all reporting companies, the CF Guidelines may have an unintended effect on publicly traded corporations that hold government contracts. While the staff emphasized that nothing in the Guidelines requires disclosure that would compromise a company's cybersecurity, such disclosure may affect contractors participating in both

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

2 *See,* Div. of Corp. Fin., SEC, CF *Disclosure Guidance: Topic No. 2: Cybersecurity* (Oct. 13, 2011), *available by* clicking here (http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm).

3 Jim Finkle & Sarah N. Lynch, *SEC Asks Companies to Disclose Cyber Attacks,* Reuters, Oct. 13, 2011, *available by* clicking here (http://www.reuters.com/article/2011/10/14/us-sec-cyberattacks-idUSTRE79C7PE20111014) (last visited Oct. 31, 2011).

4 A prior Arnold & Porter Advisory provides an in-depth discussion of the proposed bills. *See Proposed Federal Cybersecurity Legislation: A New Landscape for Regulation of Data Security and Security Breach Notifications,* (Oct. 2011) *available by* clicking here (http://www.arnoldporter.com/public_document.cfm?id=17996&key=9G0).

Contacts


Richard E. Baltz
+1 202.942.5124


Ronald D. Lee
+1 202.942.5380


Mark D. Colley
+1 202.942.5720


Caitlin Cloonan
+1 703.720.7021


Nicholas L. Townsend
+1 202.942.5249

current and future government procurements. Furthermore, government contractors will have additional disclosure obligations under rules recently proposed by the Department of Defense (DoD).

This Advisory explains the CF Guidelines relating to cybersecurity reporting obligations and discusses their import for reporting companies, with a particular focus on the negative impact that disclosure may have on reporting companies with government contracts.

Overview of the Guidelines

Reporting companies are now expected to disclose risks related to cybersecurity, including past incidents, future risks, and any foreseeable effects that cybersecurity breaches might have on a company's financial condition. The staff emphasized that the Guidelines are consistent with the relevant disclosure considerations that arise in connection with any business risk, and highlighted several areas in which disclosure of cybersecurity risk may be appropriate.

- **Risk Factors.** Disclosure of risk factors made under Item 503(c) of Regulation S-K should include the risk of cyber incidents *if these issues are among the most significant factors that make an investment in the company risky or speculative* (emphasis added). In evaluating the significance of potential cybersecurity risks, companies should consider the magnitude and frequency of past incidents and the potential costs of a cyber incident.
- **Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A).** Companies should also disclose cybersecurity risks in the MD&A section of their Form 10-K and Form 10-Q if the costs or other consequences associated with a past cyber incident or the future risks represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the results of operations, liquidity, or financial condition. Disclosure is also required to correct prior reported information that may no longer be indicative of future operating results or financial condition in light of cyber security risks or incidents.
- **Description of Business.** To the extent that cyber incidents materially affect a company's products, services, or business relationships, disclosure is required in Item 101 of Regulation S-K.
- **Legal Proceedings.** Any material legal proceedings, to which a reporting company is a party, that involve cybersecurity issues may need to be disclosed in response to Item 103 of Regulation S-K. The relevant legal proceedings of its affiliates should be included in this disclosure as well.
- **Financial Statement Disclosures.** Breaches in cybersecurity may have considerable impact on a company's financial statements depending on the nature and severity of the potential or actual incident. Effects may include, among others, losses from unasserted claims, diminished future cash flows, impairment charges, or others. Both before and after a cyber incident, companies should confirm that the costs incurred in protecting against or responding to such an incident are accounted for according to appropriate accounting standards.
- **Disclosure Controls and Procedures.** Cyber incidents may affect a company's ability to record, process, and report information to the SEC. Companies should assess risks to their reporting procedures and disclose any potential deficiencies.
- **Form 8-K.** If a cybersecurity breach occurs or new risks arise in between periodic reporting requirements, companies should consider whether disclosing such information on a Form 8-K is appropriate. Companies should disclose this information if the cyber incident or newly presented cybersecurity risk affects the accuracy and completeness of previous filings.

Implications of the CF Guidelines

In light of the CF Guidelines, reporting companies should undertake a review of the cybersecurity measures currently in place. We expect that companies will consider revising current SEC disclosures to take into account the potential risks discovered in the internal review and any past cyber incidents.

In revising disclosure documents, care should be taken not to create a "roadmap" for attacks despite SEC assurances that such detailed disclosure is not required by the Guidelines.

In the coming months, additional cybersecurity reporting requirements will likely be added to the disclosures set forth in the Guidelines. Bills being debated in the Senate would create civil penalties for failure to disclose breaches in security to those whose personal information has been compromised and criminal penalties for willful concealment of security breaches.[5] This, together with the DoD proposed rules for contractors discussed below, will create a complex web of interacting cybersecurity reporting requirements for issuers which are government contractors. At this time, it remains unclear if or when the government will reconcile these various obligations.

Disclosure Risks for Government Contractors

SEC reporting companies with DoD contracts face additional complications as a result of this increased disclosure. Periodic disclosure to the SEC of cybersecurity risks could potentially affect a company's ability to obtain future government contracts. First, when bidding on government contracts, especially contracts with significant IT requirements, competing firms could use publicly available SEC information to their competitive advantage. In addition, the government could use this information in procurement decisions. Generally, SEC disclosure is aimed at informing the market and its investors and at helping to protect companies from securities liabilities. However, such disclosures offer the government timely, credible, and accurate information regarding contractor security policies, protection, and performance. Agencies could potentially use this information to evaluate competing proposals, to assess contractor past performance and responsibility, and to evaluate and pursue potential contract claims.

The CF Guidelines are just the latest in a series of federal cybersecurity initiatives affecting government contractors. Companies performing government contracts will soon have to comply with added cybersecurity reporting requirements proposed by DoD.

On June 29, 2011, DoD issued a proposed rule (Proposed DoD Rule) to protect unclassified information shared between government and private industry. This Proposed DoD Rule would create new cyber incident reporting requirements.[6] The Proposed DoD Rule establishes two levels of information protection for nonpublic DoD information resident on, or transmitted through, a contractor's unclassified information systems: basic and heightened. Contractors with certain special handling information[7] that is subject to heightened protection would be required to file these new cyber incident reports online. A company that has access to information requiring heightened protection would have to file a cyber incident report relating to any reportable incident regardless of whether the information involved falls into one of the special handling categories. Reportable cyber incidents include those involving possible data exfiltration or manipulation or other loss or compromise of any DoD information on, or transiting through, the contractor's unclassified information systems, or any unauthorized access to an unclassified information system on which nonpublic DoD information is resident or transiting. After a cyber incident, companies would have 72 hours to report the incident to DoD.

In response to concerns by government contractors that this disclosure could be used by DoD to their competitive disadvantage, the Proposed DoD Rule includes a safeguard, albeit a narrow one, to protect government contractors

5 *See* "Personal Data Privacy and Security Act of 2011" (S. 1151); "Data Breach Notification Act of 2011" (S. 1408); "Personal Data Protection and Breach Accountability Act of 2011" (S. 1535). The text of the bills is *available* on the Senate Committee on the Judiciary's website *by* clicking here (http://judiciary.senate.gov/legislation/BusinessMeetingResults.cfm) (last visited Oct. 31, 2011). *See also* Arnold & Porter Advisory, *supra* note 4.

6 DEPT. OF DEFENSE, Proposed Rule, *Safeguarding Unclassified DOD Information, 76 Fed. Reg.* 38,089-95, (June 29, 2011) (to be codified at 48 C.F.R. pts. 204, 252).

7 The seven categories of special handling information include information bearing designations indicating controlled access, Critical Program Information, personally identifiable information, information exempt from mandatory public disclosure, and information subject to export controls under the International Traffic in Arms Regulations and the Export Administration Regulations.

from such a result.[8] However, no similar safeguard exists to prevent DoD, or any other government agency, from using the information disclosed to the public according to the CF Guidelines when making decisions regarding government contracts. Disclosure made pursuant to the CF Guidelines may actually encompass a broader range of information than conceived of under the Proposed DoD Rule, thereby giving DoD access to even more information when evaluating government contractors. This has potential consequences for reporting companies that derive a significant portion of their revenue from government contracts.

Conclusion

The CF Guidelines will require reporting companies to examine in close coordination and on a continuing basis both their cybersecurity systems and applicable disclosure documents. However, the Guidelines are only the beginning of a trend towards increased cybersecurity regulation. Arnold & Porter LLP will be monitoring the landscape for developments as they occur and can be contacted for updates.

We hope you have found this Advisory useful. If you would like more information or assistance in addressing the issues raised in this Advisory, please feel free to contact:

Richard E. Baltz
+1 202.942.5124
Richard.Baltz@aporter.com

Ronald D. Lee
+1 202.942.5380
Ronald.Lee@aporter.com

Mark D. Colley
+1 202.942.5720
Mark.Colley@aporter.com

Caitlin Cloonan
+1 703.720.7021
Caitlin.Cloonan@aporter.com

Nicholas L. Townsend
+1 202.942.5249
Nicholas.Townsend@aporter.com

Alexandra Mitter*
+1 212.715.1095
Alexandra.Mitter@aporter.com

* Not admitted to the practice of law

8 The proposed rule indicates that disclosure of cyber incidents will not automatically be considered evidence of inadequate safeguards, but DoD may consider such incidents in an overall assessment of the contractor's compliance. This is to be codified in 48 C.F.R. 204.7402(c).