Skadden

Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates

Cybersecurity: What to Expect From Proposed Legislation

A host of cybersecurity incidents this year, ranging from successful hacks into the systems of RSA, Lockheed Martin, Citigroup and Sony's Playstation Network, to McAfee's report of "Operation Shady RAT," a widespread, systematic program of cyber espionage against U.S. governmental systems by an unnamed foreign government has renewed the urgency for Congress and the Obama administration to pass comprehensive cybersecurity legislation.

We expect that Congress will come under increasing pressure to produce bipartisan legislation. Cybersecurity may be an area where both parties could come together to produce legislation. Public companies, owner/operators of "covered critical infrastructure" (*e.g.*, the energy grid, telecommunications networks, defense contractors, etc.), financial services companies, companies that collect "sensitive personally identifiable information" (such as credit card and social security numbers from consumers) and companies seeking to do business with the federal government likely would be affected by this legislation, both operationally and with respect to disclosure obligations in the event of a security breach.

The Obama administration has proposed legislation, and two separate bills have been proposed in Congress: the Cybersecurity Act of 2010 (co-sponsored by Sens. Jay Rockefeller, D-WV and Olympia Snowe, R-ME) and the Cybersecurity and Internet Freedom Act of 2011 (co-sponsored by Sens. Joseph Lieberman, I-CT, Susan Collins, R-ME and Thomas Carper, D-DE). While the content of any final legislation will differ from any of the bills' current forms, any final law may affect companies in the following general ways:

- *Cybersecurity Frameworks*: Final legislation may direct industry and government to collaborate to recognize industry-specific cybersecurity threats. Companies may be free to develop their own frameworks for mitigating these threats, with the possibility that the government would impose additional mitigation if it deems a particular company's policy insufficient.
- *Certification/Compliance Audits*: Companies may be subject to officer certification requirements and periodic commercial third-party compliance audits. Auditors would report results to the governmental authority ultimately charged with cybersecurity oversight. Where an audit reveals a company's security weaknesses, the government may require the company to implement additional security measures.
- *Contracting Requirements*: Government contractors, particularly those bidding for classified work or work in the critical infrastructure, will be at a severe disadvantage (if not barred outright) in bidding for government contracts if they fail to meet specified data security requirements or if their audit history evidences a lack of data security.

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Ivan A. Schlager
Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

Malcolm Tuesley
Washington, D.C.
202.371.7085
malcolm.tuesley@skadden.com

John P. Kabealo
Washington, D.C.
202.371.7156
john.kabealo@skadden.com

* * *

1440 New York Avenue, NW,
Washington, D.C. 20005
Telephone: 202.371.7000

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

- *Collaboration Encouragement*: Final legislation may, through liability exemptions, expertise sharing and other methods, encourage companies to seek government assistance in identifying and mitigating security weaknesses, while providing the government information to better enable it to identify systemic vulnerabilities.
- *Disclosure Obligations*: We expect final legislation to include disclosure obligations in the event of a privacy or security breach, both for public companies as well as companies that collect sensitive personally identifiable information. The threshold for triggering such an obligation and the content of the disclosure will be subject to great scrutiny as the legislative process continues.

In addition to any new legislative requirements, we expect industry "best practice" standards to become more robust. To begin preparing for more stringent requirements, companies should work with their IT and cybersecurity officers to thoroughly understand their current systems. After Congress passes legislation and agencies implement related rules, companies should seek to move swiftly to meet new requirements. We will continue to monitor the status of legislation and provide updates as significant developments occur.