MORRISON | FOERSTER

Morrison & Foerster Client Alert.

September 25, 2012

Chairman Rockefeller Requests Cybersecurity Input From Fortune 500 Companies

By D. Reed Freeman, Jr. and Nicholas Datlowe

On September 19, Senator John D. (Jay) Rockefeller IV (D-WV), chairman of the Senate Committee on Commerce, Science and Transportation, sent a letter to the CEOs of all Fortune 500 companies seeking their input on the nation's cybersecurity needs. Responses are due by Friday, October 19. Sen. Rockefeller intends to use the letter to continue his drive towards the passage of cybersecurity legislation, which faltered in the Senate last month.

Senator Rockefeller's letter states his strong belief that the Senate's failure to pass cybersecurity legislation last month leaves the country increasingly vulnerable to cyber threats. He places the blame for the filibuster that blocked the bill largely on the United States Chamber of Commerce. The purpose of the letter, he says, is to seek the unfiltered views of the nation's biggest companies on issues associated with the legislation.

In sending the letter to the CEOs, Senator Rockefeller is essentially performing an end run around the Chamber of Commerce. He states that he would be "surprised to learn" that American companies, realizing that what's good for national security is good for their bottom line, would be as "intransigently opposed" to cybersecurity legislation as the Chamber of Commerce. It is clear that the Chairman is interested in discovering the kinds of cybersecurity measures that the private sector can support in the interests of developing a comprehensive legislative solution to national cybersecurity threats.

The letter seeks responses to eight sets of questions, relating not only to corporate cybersecurity practices, but also the concerns that companies may have with the role of the federal government in establishing various cybersecurity programs. The questions are:

1. Has your company adopted cybersecurity best practices?
2. If so, how were they developed?
3. Were they developed solely within the company, or outside? If outside, by whom?

Beijing
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels
Joanna Łopatowska 32 2 340 7365
Olivier Proust 32 2 340 7360
Karin Retzer 32 2 340 7364

Hong Kong
Eric Dickinson 852 2585 0812
Gordon A. Milner 852 2585 0808

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Matthew R. Galeotti (212) 336-4044
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco
Roland E. Brandel (415) 268-7093
Anna Ferrari (415) 268-6728
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

4. When were they developed? How frequently are they updated? Are your directors or audit committee kept informed about the adoption and implementation of them?
5. Has the federal government played any role in the development of these practices?
6. What are your concerns with a voluntary program that enables the federal government and private sector to develop cybersecurity best practices?
7. What are your concerns with the federal government conducting, in conjunction with the private sector, a risk assessment to determine the nation's cybersecurity vulnerabilities?
8. What are your concerns with the federal government determining, in conjunction with the private sector, the nation's most critical cyber infrastructure?

The chairman requests responses by Friday, October 19, 2012. A copy of the letter, addressed to the CEO of IBM, can be found here. The press release accompanying the letter, including a list of all the companies to whom the letter was addressed, can be found here.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law*," or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.