Clients&FriendsMemo

The Rockefeller Letter and the Cybersecurity Debate

October 12, 2012

On September 19, 2012, Senator John D. Rockefeller IV (D-WV), Chairman of the Senate Committee on Commerce, Science, and Transportation, wrote directly to the CEOs of the Fortune 500 companies regarding cybersecurity. He solicited their views "without the filter of beltway lobbyists" and requested that they provide by October 19, 2012, answers to eight questions pertaining to their companies' cybersecurity practices and their concerns, if any, with certain aspects of the Cybersecurity Act of 2012 that failed to pass the Senate.[1] The eight questions are:

1. Has your company adopted a set of best practices to address its own cybersecurity needs?
2. If so, how were these cybersecurity practices developed?
3. Were they developed by the company solely, or were they developed outside the company? If developed outside the company, please list the institution, association, or entity that developed them.
4. When were these cybersecurity practices developed? How frequently have they been updated? Does your company's board of directors or audit committee keep abreast of developments regarding the development and implementation of these practices?
5. Has the federal government played any role, whether advisory or otherwise, in the development of these cybersecurity practices?
6. What are your concerns, if any, with a voluntary program that enables the federal government and the private sector to develop, in coordination, best cybersecurity practices for companies to adopt as they so choose, as outlined in the Cybersecurity Act of 2012?

---

[1] Letter from Senator John D. Rockefeller IV (D-WV) to Virginia M. Rometty, President and Chief Executive Officer, International Business Machines (Sept. 19, 2012), *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=396eb5d5-23a4-4488-a67c-d45f62bbf9e5.

7. What are your concerns, if any, with the federal government conducting risk assessments in coordination with the private sector, to best understand where our nation's cyber vulnerabilities are, as outlined in the Cybersecurity Act of 2012?

8. What are your concerns, if any, with the federal government determining, in coordination with the private sector, the country's most critical cyber infrastructure, as outlined in the Cybersecurity Act of 2012?

The Rockefeller letter reflects the prevailing concern that our nation is not adequately protecting its cyber infrastructure.[2] Although private industry has increased spending on cybersecurity in recent years—with one estimate placing the 2011 spending total at $80 billion[3]—one recent survey of 172 U.S. companies found that they would have to boost their cyber spending almost 900% to achieve a level of security that would stop 95% of cyberattacks.[4] Given this spending gap and the increasing reports of foreign state actors—or companies with close ties thereto—engaging in economic espionage[5] and cyberattacks,[6] it is clear that the cyber threat to American industry is very real. Indeed, Secretary of Defense Leon Panetta recently warned that the United States is facing a possible "cyber-Pearl Harbor."[7]

---

[2] This letter represents only the most recent foray by Senator Rockefeller into cybersecurity issues. For example, in May 2011, Rockefeller and four other senators wrote to Securities and Exchange Commission ("SEC") Chairman Mary Schapiro requesting that the SEC issue guidance on when companies must disclose information related to intrusions and the risks posed to their information networks. Letter from Senator John D. Rockefeller IV (D-WV) *et al.* to Mary Schapiro, Chairman, Securities and Exchange Commission, May 11, 2011, *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e. In October 2011, the SEC Division of Corporate Finance issued such guidance. *See* Cadwalader, Wickersham & Taft LLP, "The Evolving Obligations of Public Companies to Disclose Cyber-Intrusions," BUSINESS FRAUD ADVISOR, July 9, 2012, http://www.cadwalader.com/PDFs/newsletters/201207092531_BusinessFraudAdvisor_July9.pdf.

[3] Taylor Armerding, "Private Sector Fights on Despite Cybersecurity Bill's Failure," CSO ONLINE, Aug. 23, 2012, http://www.csoonline.com/article/714530/private-sector-fights-on-despite-cybersecurity-bill-s-failure.

[4] Eric Engleman & Chris Strohm, "Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps," BLOOMBERG, Jan. 31, 2012, http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html; *see also* John Hayward, "Private Sector Isn't Waiting for Feds to Deal with Internet Security," HUMAN EVENTS, Aug. 21, 2012, http://www.humanevents.com/2012/08/21/private-sector-isnt-waiting-for-feds-to-deal-with-internet-security/.

[5] Jay Greene, "Lawmakers Frustrated by Huawei, ZTE During Hearings," CNET, Sept. 13, 2012, http://news.cnet.com/8301-1035_3-57512430-94/lawmakers-frustrated-by-huawei-zte-during-hearings/.

[6] Ellen Nakashima, "Iran Blamed for Cyberattacks on U.S. Banks and Companies," WASH. POST, Sept. 21, 2012, *available at* http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html?wprss=rss_world.

[7] Elisabeth Bumiller & Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," N.Y. TIMES, Oct. 11, 2012, *available at* http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

I. The State of Cybersecurity Legislation and Regulation

Senator Rockefeller's letter reflects his frustration with Congress' inability to pass legislation to address that threat, and the questions he poses go to the core issues in the Congressional debate over that failed legislation: whether and to what extent the federal government should be involved (a) in setting minimum cybersecurity standards and (b) in asking companies to submit cyber information to the federal government. To appreciate the concerns underlying Senator Rockefeller's letter, it is important to understand the evolution of the cybersecurity debate that has played out over the past year.

Proposed Legislation

The debate started with the proposal by Senators Lieberman, Collins, Rockefeller, and Feinstein of the Cybersecurity Act of 2012. This proposed legislation would have addressed both the standard-setting and information-sharing issues.

Cybersecurity Standards: When introduced in February 2012, the original Cybersecurity Act called for the federal government to develop and impose mandatory cybersecurity standards on owners and operators in critical infrastructure industry sectors.[8] Citing their projected costs on the private sector, the bill's opponents pressed the Senate to forgo mandatory standards, and supporters of the Act ultimately agreed to make the cybersecurity standards voluntary.[9] Concerns persisted, however, that the "voluntary" standards could become mandatory in practice, and the bill ultimately failed to obtain the 60 votes needed to end debate.

Information Sharing: The original Cybersecurity Act called for industry to share certain types of cyber information with the federal government. The Act classified cybersecurity-related information into four categories: (i) information related to cyber incidents and intrusions; (ii) information related to government-conducted risk assessments; (iii) information related to performance evaluations; and (iv) information related to cyber threats. Depending on the category of cyber information, the Act required mandatory or voluntary information sharing. It required critical infrastructure owners and operators covered by the Act to report cyber intrusions and incidents to the government.[10] It required companies subject to cybersecurity performance requirements to provide information that the Department of Homeland Security ("DHS") could use to conduct risk assessments and evaluate company compliance.[11] It did not require the sharing of cyber threat information,[12] but rather

[8] S. 2105, 112th Cong. § 105 (2012).

[9] S. 3414, 112th Cong. § 103 (2012).

[10] S. 2105, § 105(b)(1)(D).

[11] S. 2105, §§ 101(b), 105(d)(3)(A), 107(a)(1); S. 3414, § 102(a)(1)(B).

provided that such information could be provided voluntarily to the government or other private sector actors.[13]

The revised Cybersecurity Act maintained the same four categories, but only required the reporting of "significant cyber incidents" to the government.[14] Information sharing related to the other three categories could be provided on a voluntary basis.[15]

Potential Executive Order

With the failure of the Cybersecurity Act, the debate has now shifted to the Executive Branch. In recent weeks, Senator Rockefeller and other members of Congress have urged the Obama administration to issue an executive order that could achieve some of the same ends as the Cybersecurity Act.[16] Last month, Secretary of Homeland Security Janet Napolitano testified that the Administration is "close to completion" of such an order.[17]

According to press reports, the draft order closely mirrors the final version of the proposed Cybersecurity Act, with its largely voluntary program for cybersecurity standards and information sharing.[18] In terms of standard-setting, a DHS-led cybersecurity council would develop guidance that would be used in the drafting of standards by industry representatives in collaboration with the National Institute of Standards and Technology ("**NIST**").[19] DHS would then work with the various sector coordinating councils—comprised of owners and operators from each particular sector of

---

[12] *See* S. 2105, § 708(6); S. 3414, § 708(7). Both versions of the Cybersecurity Act referred to this information as "cybersecurity threat indicators," which is information related to "the actual or potential harm caused by an incident," "malicious reconnaissance," technical vulnerabilities, and methods of defeating the control of an information system, among other areas. Under both versions, businesses must make "reasonable efforts" to remove personally identifiable information from the cybersecurity threat indicators.

[13] S. 2105, §§ 702(a), 704(a); S. 3414, §§ 702(a), 704(a).

[14] S. 3414, § 102(b)(4). The term "significant cyber incident" is defined as "an incident resulting in, or an attempt[] to cause an incident that if successful, would have resulted in: the exfiltration of data that is essential to the operation of critical cyber infrastructure; or the defeat of an operational control or technical control . . . essential to the security or operation of critical cyber infrastructure." S. 3414, § 2(24).

[15] S. 3414, § 102(a)(1); S. 3414, §§ 702(a), 704(a).

[16] Taylor Armerding, "Executive Order Would Not Allow 'Meaningful Leap' on Cybersecurity," CSO ONLINE, Sept. 5, 2012, http://www.csoonline.com/article/715417/executive-order-would-not-allow-meaningful-leap-on-cybersecurity.

[17] Jennifer Martinez, "Napolitano: Executive Order on Cybersecurity is 'Close to Completion'," THE HILL, Sept. 19, 2012, *available at* http://thehill.com/blogs/hillicon-valley/technology/250371-napolitano-white-house-draft-cyber-order-qnear-completionq.

[18] Jason Miller, "White House Draft Cyber Order Promotes Voluntary Critical Infrastructure Protections," FEDERAL NEWS RADIO, Sept. 7, 2012, http://www.federalnewsradio.com/241/3026867/White-House-draft-cyber-order-promotes-voluntary-critical-infrastructure-protections.

[19] *Id.*

critical infrastructure[20]—to determine which critical infrastructure sectors should be covered and which of the standards each sector would choose to impose on itself.[21] Each company in that industry sector would then be left with discretion to decide how it will meet the adopted voluntary standards.

In addition to prescribing this standard-setting process, the draft order will reportedly encourage information sharing and affirmatively "ask industry to voluntarily submit cyber threat information to the government."[22]

Concerns with the Potential Executive Order

There is concern that these "voluntary" standards could still become compulsory in several different ways. First, the Executive Branch already has statutory authority to impose mandatory guidelines that it could apply to cybersecurity in certain sectors.[23] For example, the Transportation Security Administration has authority to issue mandatory pipeline-security guidelines that could easily be applied to the cyber realm. The Executive Branch could also issue mandatory cybersecurity standards for port communication systems (regulated by the U.S. Coast Guard) and freight and passenger railroad operations (regulated by the Federal Railway Administration).[24] Or, the SEC could issue a rule requiring publicly traded companies to disclose information related to their cybersecurity practices.

---

[20] The term "critical infrastructure" is defined in section 1016(e) of the USA PATRIOT Act (42 U.S.C. § 5195c(e)) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction or such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Under the Homeland Security Act of 2002, DHS was tasked with developing a comprehensive national plan to secure critical infrastructure. *See* Homeland Security Act of 2002, Pub. L. No. 107-296, § 201(d)(5), 116 Stat. 2135, 2146. The White House issued further guidance through Homeland Security Presidential Directive 7, which identified 17 critical infrastructure sectors needing protection. DHS released the National Infrastructure Protection Plan in 2006 to coordinate efforts to protect those sectors. There are currently 18 critical infrastructure sectors. "Critical Infrastructure Sectors," DEP'T OF HOMELAND SEC., http://www.dhs.gov/critical-infrastructure-sectors (last visited Oct. 9, 2012).

[21] Jennifer Martinez, "White House Circulating Draft of Executive Order on Cybersecurity," THE HILL, Sept. 6, 2012, *available at* http://thehill.com/blogs/hillicon-valley/technology/248079-white-house-circulating-draft-of-executive-order-on-cybersecurity.

[22] Miller, "White House Draft Cyber Order Promotes Voluntary Critical Infrastructure Protections."

[23] Ellen Nakashima, "White House Drafting Standards to Guard U.S. Against Cyberattack, Officials Say," WASH. POST, Sept. 7, 2012, *available at* http://www.washingtonpost.com/world/national-security/white-house-drafting-standards-to-guard-us-against-cyberattack-officials-say/2012/09/07/0fbb173e-f8fe-11e1-a073-78d05495927c_story.html. Senator Joseph Lieberman (I-Conn.), one of the sponsors of the Cybersecurity Act of 2012, called upon the Administration last month to draft the executive order to allow federal departments and agencies to make the cybersecurity standards adopted by DHS mandatory for regulated companies. Jennifer Martinez, "Lieberman Pushes for Mandatory Standards in White House Cyber Order," THE HILL, Sept. 24, 2012, *available at* http://thehill.com/blogs/hillicon-valley/technology/251345-lieberman-pushes-for-mandatory-standards-in-white-house-cyber-order.

[24] Nakashima, "White House Drafting Standards to Guard U.S. Against Cyberattack, Officials Say."

A number of commentators have also expressed the concern that this voluntary program could quickly become compulsory by the government's use of "incentives" that would pressure companies to adopt minimum standards. One can think of myriad ways that this could be accomplished. Federal agencies could adopt a procurement preference for companies "certified" under a voluntary program.[25] Or, the government could publish a list of those companies that comply with the voluntary standards and those that do not—thereby incentivizing companies to get on the right list and avoid the "name and shame" reputational impact of being on the wrong list.[26]

Given the Administration's stated goal of setting cyber standards and information-sharing protocols, and the various levers and pressure points they can use to accomplish that goal, we should expect to see both concepts included in any proposed legislation or regulation that emerges in the near future.

II. Key Open Questions

Any comprehensive cybersecurity legislation or regulation must tackle a number of key issues, all of which raise challenging questions.

---

[25] *See* S. 3414, § 104(c)(6) (instructing the Federal Acquisition Regulatory Council to conduct a study "examining the potential benefits of establishing a procurement preference for the Federal Government for certified owners").

[26] Cybersecurity experts and industry leaders have also expressed several general concerns that Congress's focus on standards may not necessarily lead to effective security. First, given how quickly cybersecurity threats evolve there is the concern that any standards—either mandatory or voluntary—could very well be outdated before they have even been issued. Additionally, experts worry that standards setting a compliance "floor" would quickly become the "ceiling," and that program participants will focus on complying with government regulations to the detriment of a more comprehensive cyber defense effort. Finally, there is the reality that more than compliance is needed to ensure that networks are protected from intrusion and disruption. As some experts have argued, standards will be useful only "in the margins" and companies may well have to adopt more aggressive tactics—such as using the services of "digital Blackwaters" that can turn the tables and take the digital fight to the intruders—to keep cyber threats at bay. *See* Brian Prince, "Obama Cybersecurity Executive Order Nears Completion as Legislative Saga Continues," DARK READING, Sept. 21, 2012, http://www.darkreading.com/advanced-threats/167901091/security/news/240007817/obama-cybersecurity-executive-order-nears-completion-as-legislative-saga-continues.html; Pete Kasperowicz, "House Approves Second Cybersecurity Bill," THE HILL, Apr. 26, 2012, *available at* http://thehill.com/blogs/floor-action/house/224139-house-approves-second-cybersecurity-bill; Richard Stiennon, "There is No Need for a Cybersecurity Executive Order," FORBES, Sept. 8, 2012, http://www.forbes.com/sites/richardstiennon/2012/09/08/there-is-no-need-for-a-cybersecurity-executive-order/ ("Forcing utility operators, banks, and earth resources companies to comply with frameworks based on outmoded asset and vulnerability methodologies will distract them from implementing threat based defenses."); Ellen Nakashima, "Cybersecurity Should be More Active, Official Says," WASH. POST, Sept. 16, 2012, http://www.washingtonpost.com/world/national-security/cybersecurity-should-be-more-active-official-says/2012/09/16/dd4bc122-fc6d-11e1-b153-218509a954e1_story.html; Andrew Nusca, "Hayden: 'Digital Blackwater' May Be Necessary for Private Sector to Fight Cyber Threats," ZDNET, Aug. 1, 2011, http://www.zdnet.com/blog/btl/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/53639.

1. Standard Setting. Although many in Congress and the Administration prefer mandatory standards,[27] they appear to have conceded that any cybersecurity program standards created by executive order or legislation will be voluntary.[28] Even this compromise, however, will face stiff opposition. For instance, the U.S. Chamber of Commerce, which appeared initially receptive to an incentive-based approach,[29] now contends that standards created even under a voluntary program "could be used to impose new obligations on participating companies."[30]

2. Information Sharing. Private industry and various lobbying groups have expressed a variety of concerns over any program that entails the sharing of threat and vulnerability information between the government and the private sector. First, as a general matter, companies worry that information sharing will be a one-way street, with considerably more information flowing to the government than to private industry. Second, companies worry that without sufficient liability protections, they could be subject to litigation for sharing certain protected customer information or for failing to share information about a threat that results in some actionable harm. Third, private companies have cited antitrust concerns about sharing information within their industry. And finally, advocacy groups worry about the privacy implications of this information sharing with the government.[31]

---

[27] *See* Office of Mgmt. & Budget, Statement of Administration Policy, S. 3414 – Cybersecurity Act of 2012 (July 26, 2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saps3414s_20120726.pdf.

[28] Supporters of mandatory standards are not optimistic that a voluntary program will enhance cybersecurity. As one proponent of regulation in this area who had not seen the draft order noted, "Find me a company that says 'I'm going to voluntarily agree to be regulated by DHS.' Nobody is going to volunteer to have DHS regulate them." Martinez, "White House Circulating Draft of Executive Order on Cybersecurity."

[29] U.S. CHAMBER OF COMMERCE ET AL., IMPROVING OUR NATION'S CYBERSECURITY THROUGH THE PUBLIC-PRIVATE PARTNERSHIP, 10–11 (2011), *available at* http://www.uschamber.com/sites/default/files/issues/defense/files/2011cybersecuritywhitepaper.pdf (expressing a preference for an incentives-based approach and noting that such incentives could include the creation of an R&D tax credit, providing grant funding, or the establishment of a reinsurance program to stimulate the creation of a private cybersecurity insurance market).

[30] Letter from R. Bruce Josten, Executive Vice President, Government Affairs, U.S. Chamber of Commerce, to the Members of the United States Senate (July 25, 2012), *available at* http://image.uschamber.com/lib/fef61d79756700/m/1/120725+KV+S+3414+CybersecurityActOf2012+Senate+docx.pdf.

Indeed, the revised version of the Cybersecurity Act of 2012 still gave federal agencies "with responsibilities for regulating the security of critical infrastructure" the authority to adopt cybersecurity practices developed through the DHS-led public-private partnership as "mandatory requirements." S. 3414, § 103(g)(1)(A).

[31] *See, e.g.*, Rainey Reitman, Electronic Frontier Foundation, "Victory Over Cyber Spying," Aug. 2, 2012, https://www.eff.org/deeplinks/2012/08/victory-over-cyber-spying; Michelle Richardson, American Civil Liberties Union, "New Cybersecurity Amendments Unveiled to Address Privacy Concerns," July 19, 2012, http://www.aclu.org/blog/national-security-technology-and-liberty/new-cybersecurity-amendments-unveiled-address-privacy.

3. Liability Protection. Congress, the Administration, and the private sector frequently identify liability protection as a key incentive to encourage companies to adopt cybersecurity standards or engage in sharing information related to cyber threats.[32] The Obama administration has indicated, however, that any executive order will include no liability protections, as only Congress, through legislation, has the power to provide such protections.[33]

4. Definition of Critical Infrastructure. Under both the revised Cybersecurity Act and, reportedly, the Obama administration's draft executive order, the DHS-led cybersecurity council would have the authority to identify "critical cyber infrastructure" sectors which would be subject to the standards and information-sharing protocols. Critics are concerned that DHS will apply that term liberally,[34] and press reports suggest that the executive order might adopt an even broader view of critical infrastructure than that contemplated by the terms of the Cybersecurity Act.[35]

Each of these issues will figure prominently in any debate that will surely follow the issuance of an executive order or the introduction of new cybersecurity legislation.

III. Responding to Senator Rockefeller's Letter

It is important that companies keep this background and the political context in mind when deciding how to respond to Senator Rockefeller's letter.[36] They should also remember that their responses may be released to the public and that they must therefore strike a careful balance between

---

[32] Industry leaders and commentators, however, have criticized the liability protection measures under the Cybersecurity Act as insufficient. The revised bill only gave protections to "certified owners" of critical cyber infrastructure—not operators—and limited that protection to claims for punitive damages directly caused by an incident related to a risk identified through an assessment conducted under the program, as long as the owner was in "substantial compliance" with the program's security standards. S. 3414, § 104 (c)(1)(A).

[33] Jennifer Martinez, "Napolitano: Executive Order on Cybersecurity is 'Close to Completion'," THE HILL, Sept. 19, 2012, *available at* http://thehill.com/blogs/hillicon-valley/technology/250371-napolitano-white-house-draft-cyber-order-qnear-completionq.

[34] *See* Taylor Armerding, "Obama's Exec Order Draft on Cybersecurity Stirs Debate," CSO ONLINE, Sept. 14, 2012, http://www.csoonline.com/article/716187/obama-s-exec-order-draft-on-cybersecurity-stirs-debate.

[35] One reporter who has seen a copy of the draft states that DHS would be tasked with providing a report to the President "detailing the critical infrastructure that if attacked would threaten the lives of citizens or the national security of the country," which could be a broader category of critical infrastructure than would have been subject to the Cybersecurity Act. Miller, "White House Draft Cyber Order Promotes Voluntary Critical Infrastructure Protections."

[36] Companies in receipt of the letter are under no obligation to respond, but as Senate Commerce Committee spokesman Vincent Morris stated, "When a member of Congress sends a letter asking for information, the assumption is that the letter will be responded to." Siobhan Gorman, "Senator Presses on Cybersecurity," WALL ST. J., Sept. 19, 2012, *available at* http://online.wsj.com/article/SB10000872396390443720204578004690006299614.html.

providing complete and accurate responses and ensuring that they do not release sensitive business or propriety information that could be damaging to them or third parties.

* * * *

If you are in receipt of Senator Rockefeller's letter and have questions about how to respond, please feel free to contact Partner and Co-Chair of the Business Fraud and Complex Litigation Group Ken Wainstein (ken.wainstein@cwt.com, (202) 862-2474) or Associate Keith Gerver (keith.gerver@cwt.com, (202) 862-2381).