JONES DAY

JULY 2013

THE CYBERSECURITY DEBATE: VOLUNTARY VERSUS MANDATORY COOPERATION BETWEEN THE PRIVATE SECTOR AND THE FEDERAL GOVERNMENT

A REVIEW OF ATTEMPTS AT CYBERSECURITY LEGISLATION AND THE OBAMA ADMINISTRATION'S ADMINISTRATIVE ACTIONS

Cyber attacks and security breaches have become an increasingly significant risk of doing business. During the first quarter of 2013, numerous social media sites and iconic news media outlets, including Facebook, Twitter, *The New York Times*, and *The Wall Street Journal*, announced incidents of targeted cyber attacks that put the privacy of their customers at risk.[1] Criminal groups have learned that there is money to be had in the "profession" of cyber hacking. Cybercrime is now a multimillion-dollar industry serving those interested in buying and selling stolen personal data.[2] The impact on businesses is staggering: In 2012, cybercrimes cost U.S. companies an average of $8.9 million.[3] When factoring in, among other things, cybersecurity insurance, lost business opportunities, lawsuits, and mitigating adverse publicity, costs can quickly accrue. As a result, some companies have also seen the merits of enlisting well-intentioned hackers to identify system vulnerabilities. In 2012, Google announced that it was willing to pay up to $1 million in rewards to those who were able to hack its Google Chrome browser.[4] The well-known search engine explained that it wanted to test Google Chrome's strength against cybercrime and identify any existing security flaws that could be fixed.[5]

An absence of federal legislation and cybersecurity infrastructure has forced companies like Google to resort to such unusual measures in the war against cyber attacks and cybercrime. While most companies understand that their value is oftentimes tied to how well they keep consumers' information secure, they have, for years, been awaiting Congress' action in implementing heightened private sector/public sector cooperation and even cybersecurity regulation—that will not leave them bankrupt in the process. For the past several years, Congress has been unsuccessful in its attempts to adopt cybersecurity legislation that appeases both the corporate community and civil liberty groups. A heated debate has arisen concerning the best ways to regulate cybersecurity. While companies welcome input from the government about cybersecurity issues and efforts to combat cybercrime, they cringe at the notion of reporting obligations and mandates that require them to purge personal user information before sharing data concerning cybercrime threats with government entities. Instead, companies are demanding immunity from civil suits stemming from the disclosure of personal information during mandatory information sharing. Business owners are also weary of government involvement in the creation and implementation of business practices. On the other side of the debate lie technology-focused lobbying groups that dislike the promotion of information sharing without the burden of first cleansing data of all personal user information. They also reject the idea of an internet "kill switch" that would give government the power to shut down the internet in the event of a national emergency.

For years, Congress has failed to resolve the mandatory regulation versus voluntary cooperation debate. As a result, the business community has been left with the responsibility of protecting sensitive consumer data without governmental support or direction. Many believe 2013 will be the year of passage of the first cybersecurity law. This *White Paper* provides a review of failed prior legislative efforts, starting first with the Cybersecurity Act of 2010. This *White Paper* also provides a review of the Obama administration's approach to cybersecurity without legislation, namely: the Obama administration's Executive Order on cybersecurity and the measures it is taking to share governmental information about cyber threats with the corporate community.

THE CYBERSECURITY ACT OF 2010

In April 2009, Democratic Senator John D. Rockefeller IV introduced the Cybersecurity Act of 2010. Senators Evan Bayh, Barbara Mikulski, Bill Nelson, and Olympia Snowe cosponsored the bill.[6] Senator Snowe was the only Republican among the bill's sponsors. The fairly expansive and comprehensive legislation focused on creating guidelines and regulations for cybersecurity in both the public and private sectors.[7] The proposed legislation placed significant reporting and compliance requirements on public companies and authorized the President to initiate rulemaking for "critical infrastructure information systems"—information systems considered so vital to the United States that their debilitation or destruction would have crippling effects on the nation's safety and security.[8] Further, the bill charged the President to design a comprehensive national cybersecurity emergency plan.[9] The proposed bill gave the President power to employ what would be known as an internet "kill switch" as part of the mandated cybersecurity emergency plan.[10] This "kill switch" would allow the President to shut down certain portions of the internet in cases of national emergency.[11]

The notion of the internet "kill switch" stirred opposition against the bill, creating concerns that it gave the President too much discretionary power and infringed on civil liberties.[12] Critics also argued that the bill required an unwarranted increase in government spending and contained a number of measures that were both disruptive and detrimental for the cybersecurity industry.[13] The reporting and compliance requirements on the private sector were also feared to have the same effect as the "security frameworks" provision in Sarbanes-Oxley, which burdened publicly traded companies with extensive documentation and expenses related to ensuring compliance.[14] As a result of these reporting requirements, the private sector believed it was being overregulated and underfunded. In the end, the bill never received

widespread support and ultimately died in the Senate Commerce, Science, and Transportation Committee.[15]

THE PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010

On June 10, 2010, Independent Senator Joe Lieberman of Connecticut introduced the Protecting Cyberspace as a National Asset Act of 2010.[16] The bill was cosponsored by Democratic Senator Thomas Carper and Republican Senator Susan Collins.[17] The proposed legislation again directed the President to create a cybersecurity emergency plan that included the authority to seize control of, or even shut down, portions of the internet.[18] In an effort to allay fears that the bill provided the same controversial discretionary power for a presidential "kill switch" as that described in the Cybersecurity Act of 2010, Senators Lieberman and Collins issued a press release stressing that the bill only affected critical infrastructures—not the entire scope of the internet.[19] The press release failed to subdue critics' concerns, who warned that the bill created the potential for absolute power.[20]

The proposed legislation also required private companies, like broadband providers, search engines, and software firms, to comply with any emergency measures established by the Department of Homeland Security. Failure to comply meant facing hefty fines.[21] In addition, the new bill called for improvement to the nation's cybersecurity framework by establishing national committees on cybersecurity.[22] It also directed the President to appoint a single director of cybersecurity to oversee infrastructure implementation and national policy.[23]

What most differentiated this bill from its predecessor was its focus on business protections. The bill granted companies immunity from civil suits when they could show that a federal regulation or command caused a programming error that resulted in damage to customers.[24] Companies would also receive indemnification from the federal government when the harm caused to customers was the result of a federal emergency order.[25]

This time, the need for greater regulation in the private sector contributed to the bill's failure. In an effort to avoid the backlash against the reporting requirements contained in the Cybersecurity Act of 2010, the new bill shifted much of the burden from the private sector to the public sector by creating regulations and requirements that affected only the federal government.[26] While the bill tried to alleviate the financial burdens that would be placed on private industry, it was then criticized for leaving the private sector underregulated. Critics again attacked Congress for its failure to find a "sweet spot" between the business community and privacy interests.

Critics, including the nation's largest technology-focused lobbying group, were also focused on the possibility of another internet "kill switch."[27] Despite receiving bipartisan support from Democratic Representative Jay Rockefeller and Republican Representative Olympia Snowe, the bill failed to gain widespread support.[28]

INTERNATIONAL CYBERCRIME REPORTING AND COOPERATION ACT

The International Cybercrime Reporting and Cooperation Act was introduced by Democratic New York Senator Kirsten Gillibrand in August 2011.[29] Gillibrand's proposed legislation focused on cybersecurity efforts overseas as it addressed multilateral efforts to prevent and investigate cybercrime on an international level.[30] The bill required the President to provide an annual presidential report to Congress that discussed foreign countries' use of information and communications technologies ("ICT") and their responses to cybercrime on a domestic and international level.[31] The bill also promoted foreign assistance to potential cybercrime havens by requiring the President to develop programs designed to combat cybercrime abroad in countries with low ICT levels.[32] Further, the bill directed the President to identify countries of cyber concern and impose restrictions on those countries that failed to comply with appropriate benchmarks.[33]

The internationally focused bill was referred to various subcommittees, including Foreign Affairs, Ways and Means, and Financial Services, but it ultimately fell victim to subcommittee debate and, like other attempts at cybersecurity regulation, never moved past the committee stage.[34]

THE CYBERSECURITY ACT OF 2012

On February 14, 2012, Independent Senator Joe Lieberman made yet another attempt at cybersecurity legislation through the introduction of the Cybersecurity Act of 2012.[35] Republican Senator Susan Collins and Democratic Senators Dianne Feinstein, John Rockefeller, and Sheldon Whitehouse were cosponsors.[36] Unlike its predecessors, the bill's directives were aimed at federal agencies, instead of the President. The bill also aimed to protect critical U.S. infrastructure through joint collaboration between the government and the private sector.[37]

The proposed legislation directed the Secretary of Homeland Security to consult with owners of critical infrastructure and formulate an action plan to protect the nation's critical systems.[38] The bill also asked federal agencies to adopt best practices that would motivate employees to demonstrate leadership in cybersecurity.[39] Further, it required the Department of Homeland Security to coordinate with private sector and academic experts to develop risk management strategies.[40] The expansive legislation also touched on education programming. The bill required the development of new education and recruitment programs and directed the Secretary of Education to develop curriculum standards to include cybersecurity issues from elementary school through higher education.[41]

The Cybersecurity Act of 2012 encountered strong opposition from Republican senators, including Senator John McCain, who sided with the U.S. Chamber of Commerce.[42] Opponents largely consisted of business leaders, who argued that the bill's regulations intruded into private business operations, thereby increasing private sector costs.[43] While businesses believed the bill gave the government too much power in regulating their own security, supporters of the bill contended that there could be no guarantees that companies would self-regulate if left to their own devices.[44] Republicans promptly initiated a filibuster in the Senate, and thus there was never a final vote on the measure.[45]

PRESIDENT OBAMA'S EXECUTIVE ORDER: "IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY"

Frustrated with Congress' lack of progress in adopting cybersecurity legislation, President Obama identified cybersecurity among the top issues to address in his second-term agenda.[46] On February 12, President Obama issued an Executive Order titled "Improving Critical Infrastructure Cybersecurity."[47] The Executive Order was signed just hours before the President's State of the Union Address, in which he again highlighted the need for a cybersecurity framework.

The Executive Order dramatically broadened existing information sharing programs, making it easier for private companies in control of the nation's critical infrastructure to share information about cyber attacks with the government.

Section 9(a) of the Executive Order provides that within 150 days, i.e., by July 12, the Secretary of Homeland Security "shall use risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, e-commerce security, or national security." The Section includes a carve-out for "commercial information technology services." Section 9(e) provides that the Secretary is to notify confidentially the owners and operators of critical infrastructure of their designation as such and shall provide to them the basis for that determination. The owner and operators may request reconsideration.

Section 2 of the Executive Order defines the key term "Critical Infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of 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." Debates have already broken out and lobbying commenced regarding which firms will be found to provide "critical infrastructure" and which firms will be exempt "commercial information technology service" providers. For example, telecommunication service providers such as AT&T and Verizon have questioned why firms that provide digital services—such as Google, Apple, and Microsoft—should be exempted.[48] Marcus Sachs, Vice President of National Security Policy for Verizon, argues that email is "critical infrastructure": "If email went away this afternoon, we would all come to a stop. Hell yeah, email is critical."[49] Others add that it is not realistic to expect to protect telecommunications "critical infrastructure" unless information technology products that use telecommunications networks are also considered because hackers will naturally attack the weakest link in any network.

Section 7 provides that the Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Director is ordered to publish a preliminary version of the Cybersecurity Framework within 240 days, i.e., by September 30. The final version is due within one year, i.e., by February 12, 2014.

Section 8 directs the Secretary of Homeland Security to establish a "voluntary program" to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested parties. In particular, Section 8(d) directs the Secretary to "coordinate establishment of a set of incentives designed to promote participation in the program." Section 8(e) provides that the Secretary of Defense and Administrator of General Services, in consultation with the Secretary of Homeland Security and the Federal Acquisition Regulatory Council, shall make recommendations to the President and others "on the feasibility, security benefits and relative merits of incorporating security standards, into acquisition planning and contract administration."

Under Section 10(a), within 90 days of publication of the preliminary Cybersecurity Framework, i.e., by December 29, various federal agencies are directed to issue a report to the President "that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required." Under Section 10(b), if current regulatory requirements are deemed insufficient, then within 90 days of the publication of the final Cybersecurity Framework, i.e., by May 13, 2014, the agencies are directed to propose risk-based, efficient and coordinated actions to mitigate cyber risks. Under Section 10(c), within two years after the publication of the final Cybersecurity Framework, the agencies are directed, "in consultation with owners and operators of critical infrastructure, [to] report to CMB or any critical infrastructure subject to ineffective, conflicting or excessively burdensome cybersecurity requirements."

In an effort to address the fact that Executive Orders generally lack any actual legal enforcement, President Obama offered incentives to companies to voluntarily adopt the standards initiated under the Cybersecurity Framework.[50] Despite this work-around, critics argued that the Executive Order failed to provide companies with sufficient protections that would induce any voluntary cooperation.[51] Private companies willing to participate faced a significant risk: Information sharing with the government could lead to additional liabilities and lawsuits because the data that would be given to the federal government could include private information from customers. As a result, critics questioned whether companies will participate without additional protections and safeguards, such as legal immunity from civil suits.[52] Regardless, analysts predicted that the President's Executive Order would serve as the starting point for congressional action on meaningful cybersecurity legislation.[53]

CISPA

On February 12—the very same day that President Obama issued his Executive Order on cybersecurity—Republican Representative Mike Rogers and Democratic Representative Dutch Ruppersberger introduced the Cyber Intelligence Sharing and Protection Act ("CISPA").[54] The proposed bill required the Director of National Intelligence to establish procedures that would allow the federal government, including the intelligence community, to share cyber threat information with the private sector.[55] Upon receipt of such information, private entities would thereafter be prohibited from further disclosure of the cyber threat information to third parties.[56] The bill also allowed companies to pass user information to the federal government and absolved private sector firms of the responsibility or requirement to remove personal information before sharing it with the government.[57] Further, CISPA provided broad legal immunity to companies that collected and shared inaccurate cyber threat information, as long as they were able to prove that the information was provided in good faith.[58]

Allowing companies to pass unsanitized user information to the government, however, stirred significant outcry from civil liberty groups, which argued that the bill could lead to significant violations of privacy rights.[59] The broad grant of immunity to cooperating companies also initiated opposition from the White House.[60] The administration argued that the scope of liability protections granted to businesses was too broad and that more targeted liability protections were needed.[61] On April 18, the House of Representatives passed CISPA with a vote of 288–127, despite strong opposition from privacy advocate groups and a veto threat from the White House.[62]

Currently, CISPA's future looks grim as it sits stalled in Senate subcommittee. Privacy rights lobbying groups and internet activists have come together in strong opposition of the bill, declaring a violation of privacy rights.[63] Outspoken Democratic senators, like Jay Rockefeller of West Virginia, have vowed to fight the bill and prevent its passage. Understanding and accepting the bill's likely demise, both Senator Jay Rockefeller and Georgia Republican Senator Saxby Chambliss have decided to "start from scratch," and are working on new legislation aimed at bridging the gap between corporate interests and privacy rights.[64]

While legislators continue to search for the seemingly elusive balance between effective cybersecurity regulation, business interests, and privacy protections, businesses are left to fend off cybercrimes on their own. As cybercrimes increase, businesses will be forced to focus their attention and resources on collateral business obligations, rather than the promotion of their respective services and products. Google illustrates one of the most innovative ways in which to engage the battle against cybercrime, and it also underscores the importance of cybersecurity. In an effort to avoid the unwanted costs and distractions associated with data breaches, businesses must now make it a priority to be vigilant in their efforts to combat cybercrime. The first steps in establishing proper cyber protections should begin with conducting risk assessments to identify system vulnerabilities. Identifying internal weaknesses will assist businesses in establishing internal policies and protections that will strengthen their security measures and fortify their data.

Further attempts at passing cybersecurity legislation are expected for the remainder of 2013. In order to successfully do so, Congress will need to offer substantive guidance to those businesses seeking ways to improve their cybersecurity without overstepping in internal business management and day-to-day operations. Further, it will need to find equilibrium between business interests and privacy protections. Until effective cybersecurity legislation comes to fruition, businesses must understand that it is up to them to protect their consumers, and their ultimate bottom line.

BANKING REGULATORS URGE BANKS TO TAKE ACTION

U.S. regulators are not waiting on Congress to take action to combat cyber attacks. For example, federal officials and the banking industry are preparing for a major cyber "war game" exercise titled "Quantum Dawn 2" involving banking regulators, the Department of Homeland Security, and major banks and securities firms represented by the Securities Industry and Financial Management Association.[65] Moreover, Treasury Department officials and other officials have been conducting classified and nonclassified briefings with bank officials.[66] Finally, federal financial regulators are advising bank executives to change the way they think about cyber attacks and to consider them as they do more traditional risks, such as credit and interest rate risk, when they make strategy decisions. Taking it a step further, federal regulators are telling banks that they will be judged on their preparations against cyber attacks when regulators evaluate their operational risks.[67]

CONCLUSION

The advice and warnings that federal financial regulators are now providing to bank executives should be heeded by all private sector firms. While the private sector should remain involved in congressional attempts to pass cybersecurity legislation, it should not wait on legislation to take action. The risks are simply too great.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Jean-Paul Boulee
Atlanta
+1.404.581.8456
jpboulee@jonesday.com

Walter W. Davis
Atlanta
+1.404.581.8517
wwdavis@jonesday.com

Robert W. Kantner
Dallas
+1.214.969.3737
rwkantner@jonesday.com

Kristen Pollock McDonald
Atlanta
+1.404.581.8498
kmcdonald@jonesday.com

Janine C. Metcalf
Atlanta
+1.404.581.8656
jmetcalf@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Katherine S. Ritchey
San Francisco
+1.415.875.5728
ksritchey@jonesday.com

Richard J. Johnson
Dallas
+1.214.969.3788
rjohnson@jonesday.com

Natalie A. Williams, an associate in the Atlanta Office, assisted in the preparation of this White Paper.

ENDNOTES

1 Joanna Stern, "Facebook Hacked; No User Data Compromised," ABC News, Feb. 15, 2013, http://abcnews.go.com/Technology/facebook-hacked-month-user-data-compromised/story?id=18515870#.UYFVeKK-1Bk; Dan Milano, "250,000 Twitter Accounts Hacked: Don't Panic, Here's What to Do," ABC News, Feb. 1, 2013, http://abcnews.go.com/blogs/technology/2013/02/250000-twitter-accounts-hacked-dont-panic-heres-what-to-do; Jethro Mullen, "New York Times, Wall Street Journal Say Chinese Hackers Broke into Computers," *N.Y. Times*, Jan. 31, 2013, http://www.cnn.com/2013/01/31/tech/china-nyt-hacking; Nicole Perlroth, "Wall Street Journal Announces That It, Too, Was Hacked by the Chinese," *N.Y. Times*, Jan. 31, 2013, http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html?_r=0.

2 David Goldman, "Cybercrime: A Secret Underground Economy," *CNN Money*, Sept. 17, 2009, http://money.cnn.com/2009/09/16/technology/cybercrime.

3 *2012 Cost of Cyber Crime Study: United States* (Ponemon Institute, Working Paper, October 2012) http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

4 Andy Greenberg, "Google Will Offer $1 Million in Rewards for Hacking Chrome in Contest," *Forbes*, Feb. 28, 2012, http://www.forbes.com/sites/andygreenberg/2012/02/28/google-will-offer-1-million-in-rewards-for-hacking-chrome-in-contest; *see* "The Digital Arms Race," *The Economist*, March 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade.

5 Greenberg, *supra* note 4.

6 The Cybersecurity Act of 2010, S. 773, 111th Cong. (2010).

7 *Id.*

8 *Id.* §§ 3-4.

9 *Id.* § 201(b).

10 *Id.* § 18.

11 *Id.*

12 Jeremy A. Kaplan, "New Cybersecurity Act Eliminates Internet Kill Switch," FoxNews, Mar. 18, 2010, http://www.foxnews.com/tech/2010/03/18/obama-no-longer-internet-president/; *see* Jon Stokes, "President's Veto Power Over Internet Removed in Amended Bill," *Ars Technica*, March 22, 2010, http://arstechnica.com/tech-policy/2010/03/presidents-veto-power-over-internet-removed-in-amended-bill.

13 Richard Stiennon, "Rockefeller's Cybersecurity Act of 2010: A Very Bad Bill," *Forbes*, May 4, 2010, http://www.forbes.com/sites/firewall/2010/05/04/rockefellers-cybersecurity-act-of-2010-a-very-bad-bill.

14 *Id.*

15 *See* S. 773, http://thomas.loc.gov/cgi-bin/bdquery/z?d111:SN00773:@@@L&summ2=m& (accessed March 26, 2013).

16 Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. (2010).

17 *Id.*

18 Bianca Bosker, "Internet 'Kill Switch' Would Give President Power to Shut Down the Web," *The Huffington Post*, June 17, 2010, http://www.huffingtonpost.com/2010/06/17/internet-kill-switch-woul_n_615923.html; Declan McCullagh, "Senators Propose Granting President Emergency Internet Power," CNET, June 10, 2010, http://news.cnet.com/8301-13578_3-20007418-38.html.

19 Press Release, United States Senate Committee on Homeland Security and Governmental Affairs, "Myth vs. Reality: The Facts About S. 3480," June 23, 2010, http://www.wired.com/images_blogs/threatlevel/2011/01/Myth-v-Reality.pdf.

20 *See* Bosker, *supra* note 18.

21 *Id*; McCullagh, supra note 18.

22 S. 3480, §§ 101-102.

23 *Id.*

24 *Id.* § 249.

25 *Id.*

26 *See* S. 3480.

27 Bosker, *supra* note 18; see McCullagh, *supra* note 18.

28 *See* McCullagh, *supra* note 18.

29 The International Cybercrime Reporting and Cooperation Act, S. 1469, 112th Cong. (2011).

30 *Id.*

31 *Id.* § 3.

32 *Id.* § 4.

33 *Id.* § 5.

34 S. 1469 (112th): International Cybercrime Reporting and Cooperation Act Summary, http://www.govtrack.us/congress/bills/112/s1469.

35 The Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012).

36 *Id.*

37 *See id.*

38 *Id.* § 202. The bill defined "covered critical infrastructure" as systems or assets that, if damaged or accessed without authorization, could reasonably lead to the interruption of life-sustaining services sufficient to cause a mass casualty event with an extraordinary number of fatalities or mass evacuation with a prolonged absence, catastrophic economic damage to the United States, or severe degradation of national security. "Catastrophic economic damage" was defined to include the failure or substantial disruption of a U.S. financial market, transportation system, or other systematic, long-term damage to the U.S. economy. Commercial information technology products were excluded.

39 *Id.* § 243.

40 *Id.* § 601.

41 *Id.* § 407(c)(2).

42 Michael Schmidt, "Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster," *N.Y. Times*, August 2, 2012, http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html?_r=0.

43 Heather Kelly, "5 Big Tech Issues Await Obama in Second Term," CNN, Nov. 14, 2012, http://www.cnn.com/2012/11/13/tech/innovation/obama-tech-policy.

44 *Id.*

45 Schmidt, *supra* note 42.

46 *See* David Goldman, "President Obama Cracks Whip on Cybercrime," CNN, Feb. 12, 2013, http://security.blogs.cnn.com/2013/02/12/president-obama-cracks-whip-on-cybercrime/?iref=allsearch.

47 Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

48 Eric Engleman, "National Security—Fighting An Order to Fight Cybercrime," *Bloomberg Business Week*, March 11-17, 2013, pp. 30-31.

49 *Id.*

50 Steve Holland, "Obama Signs Executive Order for Better Protection from Cyber Attacks," NBC News, Feb. 12, 2013, http://www.nbcnews.com/technology/obama-signs-executive-order-better-protection-cyber-attacks-1C8349540; Goldman, *supra* note 46.

51 Goldman, *supra* note 46.

52 *See Id.*

53 Arik Hesseldahl, "Obama's Cybersecurity Order Aims for a Restart with Congress," All Things D Blog (Feb. 13, 2013, 7:26 PM), http://allthingsd.com/20130213/obamas-cybersecurity-order-aims-for-a-restart-with-congress.

54 Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013). This was not the first time CISPA was introduced to the House of Representatives. Both Representatives Rogers and Ruppersberger sponsored the bill the year before. CISPA originally died in 2012 after the Senate failed to approve the bill because of looming privacy concerns.

55 Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013) § 3(a)(1).

56 *Id.* § 3(a)(5).

57 *Id.* § 3; Jason Koebler, "Lawmakers to 'Start from Scratch' After CISPA Bill is Shelved," *US News and World Report*, April 26, 2013, www.usnews.com/news/articles/2013/04/26/lawmakers-to-start-from-scratch-after-cispa-bill-is-shelved; Chenda Ngak, "As CISPA Cybersecurity Bill Passes House, Privacy Advocates Mobilize," CBS News, April 18, 2013, http://www.cbsnews.com/8301-205_162-57580334/as-cispa-cybersecurity-bill-passes-house-privacy-advocates-mobilize.

58 *Id.* § 3(b)(3)(A); Koebler, *supra* note 57.

59 Koebler, supra note 57.

60 *Id.*

61 *Id.*

62 Ngak, *supra* note 57.

63 Julian Sanchez, "CISPA is Dead. Now Let's Do a Cybersecurity Bill Right," *Wired*, April 26, 2013, http://www.wired.com/opinion/2013/04/cispas-dead-now-lets-resurrect-it/; *see Id*; Koebler, *supra* note 57.

64 Koebler, *supra* note 57.

65 Michael R. Crittendon, "A Call to Arms for Banks—Regulators Intensify Push for Firms to Better Protect Against Cyber attacks," *The Wall Street Journal*, June 15-16, 2013, B1 and B2.

66 *Id.*

67 *Id.*