Skadden

PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

05.04.12

Cybersecurity Policy Developments

Pending Legislative Action in the House; China as a Network Security Concern

As cybersecurity issues continue to garner headlines, more than half a dozen bills that attempt to address different facets of network security are pending in Congress.[1] Last week, the House of Representatives passed four separate bills addressing various aspects of the cybersecurity problem.[2] The Obama Administration has already proposed its own model bill[3] and continues to press Congress to act, citing a number of potential threats.[4] In the Senate, proponents of the leading bill are negotiating with proponents of a Republican alternative.[5] Meanwhile, perceptions of the threat continue to evolve and congressional proposals continue to change as new information becomes available. Notably, lawmakers increasingly are singling out China as the most threatening state actor, especially with respect to economic espionage.[6]

Operators of "critical infrastructure" should be aware of their potential new legal obligations and privileges under the various bills. The bills' definitions of "critical infrastructure" vary, but generally include operators of utilities and the electrical grid, telecommunications networks, financial services firms and defense contractors. Technology companies, government contractors and others also may be covered. All of these parties may face new regulatory requirements after the passage of a law. Operators of critical infrastructure and other businesses that source equipment from foreign sources, most notably China, may also be affected by a new law. Businesses also may need to update their cybersecurity policies related to the handling of sensitive business and customer information to address any new laws or regulations.

I. Cybersecurity Legislation: Latest Developments

Last week, the House of Representatives sent four separate cybersecurity bills to the Senate. While the leading Senate bill, the Cybersecurity Act of 2012 (Cybersecurity Act), takes a comprehensive approach to network security, the House has addressed several components of the Senate bill in separate pieces of proposed legislation. Three of the four House bills passed

---

1 *See David Perera, Cybersecurity Legislation Roundup, 2012 Edition*, FierceGovernmentIT, Mar. 28, 2012.
2 See House Hopeful About Cybersecurity Bill, Washington Post, Apr. 29, 2012.
3 *See* Posting of Howard A. Schmidt to the White House Blog, *The Administration Unveils its Cybersecurity Legislative Proposal* (May 12, 2011, 2:00 PM), http://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal.
4 *See* Eric Engleman and Chris Strohm, *Mock Cyber Attack on New York Used by Obama to Pitch Senate Bill*, Bloomberg, Mar. 8, 2012.
5 *See* Brendan Sasso, *House Gears Up for "Cyber Week," But Security Bill's Fate Rests with Senate*, The Hill: Hillicon Valley, Apr. 21, 2012.
6 *See, e.g.*, Mike Rogers, *CISPA Defends America from Predators*, U.S. News and World Report, Apr. 18, 2012 (Mike Rogers, author of the leading House bill: "[D]angerous economic predators, including nation-states like China, use the Internet to steal valuable information from American companies and unfairly compete with our economy"); Josh Smith, *Swan Song*, National Journal, Mar. 9, 2012 (Joe Lieberman, author of the leading Senate bill: "I've seen estimates that go into the hundreds of billions of dollars. The more significant part is this methodical theft of industrial secrets. China is not the only country doing this but is by far the largest actor").

LEARN MORE

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

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

Stuart D. Levi
New York Office
T: 212.735.2750
stuart.levi@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

Joshua F. Gruenspecht
Washington, D.C.
202.371.7316
joshua.gruenspecht@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

last week address federal agency cybersecurity, the coordination of federal research efforts, and research and development funding for the private sector.

The fourth bill, the Cyber Intelligence Sharing and Protection Act (CISPA), would remove some of the legal barriers to sharing information regarding network security threats between the government and certain private sector entities.[7] Providers of network security services to third parties would be able to request those parties' consent to share portions of their communications traffic that appear to contain threat information. Such information could then be shared with designated entities "notwithstanding any other provision of law."[8] Shared information would not be able to be used "to gain an unfair competitive advantage,"[9] those who pass that information on would be immunized from liability if they do so in good faith.[10]

Two additional House bills addressing further aspects of cybersecurity were not brought to the floor last week. The first, the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011 (PRECISE Act), has been placed on temporary hold by the House leadership pending its further evaluation.[11] The PRECISE Act is intended to present the House's alternative to the critical infrastructure regulatory framework proposed in the Cybersecurity Act. While the bill originally would have allowed the government to set security standards for critical infrastructure systems, the House Homeland Security Committee has removed those powers in the latest draft and is continuing to edit the bill in hopes of creating a version that can acquire bipartisan support.[12] The second, the Secure and Fortify Electronic Data Act (SAFE Data Act), has not yet been voted out of committee. The SAFE Data Act would preempt the current patchwork of state requirements for reporting breaches of consumers' personal data and replace them with a unified federal alternative.

Implications

Efforts to create a unified bill remain very much in flux. CISPA, the first major cybersecurity bill to pass either house of Congress, has attracted opposition from some of the same entities that successfully stalled the Stop Online Piracy Act (SOPA) earlier this year. The White House has threatened to veto the bill over its lack of "sufficient limitations" on information sharing and its failure to grant the government regulatory authority over critical infrastructure.[13] While the passage of comprehensive legislation faces significant obstacles, including policy disagreements and political differences among the House, Senate and White House as well as the general difficulty in passing significant legislation in an election year, the practical need to address the growing threat may yet spur legislative action, particularly if another high-profile cyber attack against the U.S. occurs.

Companies should note that the House leadership has come out strongly against some of the regulatory measures proposed in the Senate bills and discussed in our September update. However, the debate over the PRECISE Act and the Senate bills demonstrates continuing support for additional regulation of critical infrastructure within both parties in both houses of Congress. Companies could still face new regulatory compliance regimes and auditing or new federal standards for disclosing data breaches.

In the event that information sharing legislation passes, companies also will need to pay increasing attention to the terms on which data is shared with security vendors and cloud service providers. Because some bills propose information-sharing provisions that are not limited by any other pre-existing law — such as, for example, laws protecting against the disclosure of trade secrets — any

---

7 *See* Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. § 2(a) (as engrossed Apr. 26, 2012) (adding new 50 U.S.C. § 1104(a)-(b)).
8 *Id.* (adding new 50 U.S.C. § 1104(b)(1)).
9 *Id.* (adding new 50 U.S.C. § 1104(b)(3)(B)).
10 *Id.* (adding new 50 U.S.C. § 1104(b)(4)(A)).
11 *See* Brendan Sasso, *House to Vote on Four Cyber Bills, Leaves Out Lungren Measure*, The Hill: Hillicon Valley, Apr. 20, 2012.
12 *Id.*
13 *See* Executive Office of the President, *Statement of Administration Policy: H.R. 3523 – Cyber Intelligence Sharing and Protection Act*, Apr. 25, 2012.

(continued on next page)

information shared for cybersecurity purposes will require thorough review, contractual protections and/or sanitization.

II. U.S.-China Economic and Security Review Commission Report on Chinese Cyber Capabilities

One theme of the ongoing legislative debate has been concern over the cybersecurity threat from China. Numerous groups have raised this disquiet before Congress, including the U.S.-China Economic and Security Review Commission (the Commission), a bipartisan standing commission established to "review the national security implications of trade and economic ties between the United States and the People's Republic of China" and report its findings to Congress.[14] On March 8, 2012, the Commission released its latest report (the Report) assessing the network security threat from China.[15] The Report begins by addressing the information warfare capabilities and strategies of the Chinese military, but then turns to the threats posed by nongovernmental actors. Chinese telecommunications equipment, parts and service suppliers are assessed as a threat to U.S. interests in three different ways.

First, the Report discusses collaboration between the Chinese state and Chinese telecommunications companies. It suggests that the military increasingly has relied on "civilian universities[,] private commercial IT firms … or hundreds of smaller niche firms" as collaborators for developing military applications.[16] Second, the Report considers the much-discussed "supply chain" threat — the possibility that Chinese manufacturers selling equipment or parts to intelligence targets will place code within devices that will give Chinese military or intelligence actors a means of intercepting the communications traffic carried over those devices. It states that upstream attacks on suppliers of parts are "feasible for only extremely well-resourced organizations," but that the downstream risk from altered or counterfeit hardware replacing expected shipments is more troubling.[17] Third, the Report discusses collaboration between U.S. network security services providers and Chinese telecommunications companies. Ultimately, it concludes that the threat in that space is not immediate. Instead, it says, such partnerships could help Chinese companies gain access to the latest tools of the security trade and provide an avenue through which to sell more equipment to American firms.[18]

After releasing the Report, the Commission held a number of briefings to discuss its findings with members of Congress, congressional staff and the public. At a public hearing on March 26th, many of the panelists emphasized the need for legislative action. One former Marine Corps general stated that "the last thing [he would] want to do is demonize the Chinese" and stressed the need for intergovernmental dialogue. Others on the panels, however, suggested that the threat from Chinese telecommunications companies was so great as to require an immediate response.

Implications

Whether or not cybersecurity legislation ultimately passes, inbound investment will continue to require thorough legal, public relations and government relations planning in the current political environment. Critical infrastructure businesses such as energy and defense, businesses in regulated industries, and those that have a large number of government contracts may want to carefully review and update cybersecurity policies prior to signing significant new contracts with foreign providers of telecommunications equipment and services, or with those who source their equipment overseas. Investment from China and major contracts with Chinese providers will continue to receive particular scrutiny from government bodies.

---

14 22 U.S.C. § 7002 (2001).
15 U.S.-China Economic and Security Review Commission, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage (2012) (the "Report").
16 Report, at 68.
17 *See* Report, at 87-93.
18 *See* Report, at 103-06.