Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Senate Cybersecurity Bill Vs. House Cybersecurity Bills

Law360, New York (November 19, 2015, 10:13 AM ET) -- Cybersecurity threats reflect, as President Obama has said, that the technologies that "empower us" can also "undermine us."[1] From business to government and academia, the increasing frequency and severity of cyber events have taken a toll. This includes the pilfering of sensitive personal and financial information, leaving privacy and confidentiality in the dust and sometimes causing financial injury; the theft of confidential business information and intellectual property that has tilted the competitive playing field; the compromise of industrial control systems that has given rise to physical peril; and a wide and costly trail of compromise, damage and destruction.

There are no silver bullets to defeat these threats. There is, however, bipartisan hope that some improvement will come if information about threats is voluntarily shared much faster, before the threats can reap illicit rewards again and again. Along these lines, the president has described a "shared mission" between government and industry that extends to cybersecurity information sharing: "So much of our computer networks and critical infrastructure are in the private sector, which means government cannot do this alone. But the fact is that the private sector can't do it alone either, because it is government that often has the latest information on new threats. There's only one way to defend America from these cyberthreats, and that is through government and industry working together, sharing appropriate information as true partners."[2]

Against this background, on Oct. 27, 2015, the Senate passed the Cybersecurity Information Sharing Act (S.754, "CISA"), sponsored by Sens. Richard Burr, R-N.C., and Dianne Feinstein, D-Calif., the chairman and vice chairwoman of the Senate Intelligence Committee, by a margin of 74 to 21. The next step on the bill's challenging path is a conference committee that will seek to mesh its provisions with those of two House bills passed earlier.

Previously, on April 22, 2015, the House passed H.R. 1560, the Protecting Cyber Networks Act (PCNA), sponsored by House Intelligence Committee Chairman Devin Nunes, R-Calif, with Ranking Member Adam Schiff, D-Calif., as lead cosponsor. The bill passed by a wide margin of 307-116, and was followed a day later by passage of H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (NCPAA), by a vote of 355-63. That bill is sponsored by Homeland Security Committee Chairman Michael McCaul, R-Texas. Following the passage of the two House bills, each was enrolled as a title to a single bill in order to more easily be conferenced with CISA.

The Senate and House bills are intended to foster voluntary cybersecurity information sharing on a real-time or near real-time basis, both among companies and between companies and the government. Today, most information sharing that takes place generally is not real-time and tends to be most common only in certain critical industries, such as segments of financial services. The bills seek to encourage more and faster sharing by providing liability and certain confidentiality protections to businesses who share cybersecurity threat information, stripped of sensitive privacy information.[3]

The idea behind the bills is that businesses own much of the infrastructure and data being attacked, the government also has relevant information and insights, and that voluntary sharing, incentivized through liability protection, can help identify and defend against threats and limit the period of time and number of instances for which a particular attack can be repeated and work effectively. In part, the bills are aimed directly at general counsels, by seeking to reduce legal risks and help tip a cost-benefit analysis further in favor of voluntary information sharing. However, the Senate and House bills differ in their approach to certain issues discussed below.

Information Sharing Process

The NCPAA would require the U.S. Department of Homeland Security undersecretary for cybersecurity and infrastructure protection to develop capabilities that make use of existing industry standards to implement automated mechanisms for the sharing of cyberthreat indicators and defensive measures to and from the National Cybersecurity Communications and Integration Center (NCCIC) and with any federal agencies designated as sector specific agencies for critical infrastructure sectors (i.e., energy, agriculture, defense, transportation, etc.).

In contrast, the PCNA amends the National Security Act of 1947 to require the director of national intelligence (DNI) to develop and promulgate procedures to facilitate the sharing of classified and declassified cyberthreat indicators in the possession of the federal government with private entities. It also authorizes private entities to conduct information system monitoring activities and operate defensive measures for cybersecurity purposes, and to share or receive any cyberthreat indicators with/from other private entities or an "appropriate federal entity" (defined as the U.S. Department of Commerce, Department of Energy, DHS, Department of Justice, DNI, or Treasury Department).

A major difference between the House bills and CISA that must be resolved is the question of whether to funnel all shared data through a single agency (DHS), as CISA generally would in order to obtain liability protection for sharing with the government, or permit sharing with any of multiple agencies too, as the House bills readily allow. In contrast to the House bills, CISA would establish DHS as the "portal" through which cyberthreat information is shared and later distributed to other agencies as necessary. DHS would also be tasked with ensuring that information shared through the portal maintains personal privacy and civil liberties protections.

The White House announced support for passage of CISA, shortly before it passed. In its statement of administration policy in favor of passage, the White House stated that all private sector data should be shared through DHS to secure liability protection and that DHS could then share efficiently with other federal agencies. It also expressed concern over exceptions, stating that DHS is best suited to preserve privacy and civil liberties protections before sharing threat information with other agencies.

Privacy Protection and Removal of Personally Identifiable Information

The PCNA, NCPAA and CISA all require federal and nonfederal entities that participate in cyberthreat sharing to protect the data they collect, maintain and share from unauthorized access and disclosure.[4] Further, each bill requires the removal of personally identifiable information before a threat indicator is shared. The House bill requires that "reasonable efforts" be made to scrub such information and permits sharing where an entity "reasonably believes" they have removed the PII from threat indicators before sharing; CISA bars sharing where an entity "knows at the time of sharing" that PII is included.[5]

The PNCA and CISA direct the DOJ to promulgate and periodically review privacy and civil liberties guidelines to limit receipt, retention, use and dissemination of personal or identifying information by the federal government. The PCNA would require interim guidelines to be developed and submitted to Congress within 90 days, while CISA would require such interim guidelines to be established within 60 days (and later finalized within 180 days as with PCNA). Alternately, NCPAA would require the DHS undersecretary to establish and annually review privacy and civil liberties policies governing the receipt, retention, use, and disclosure of cybersecurity information shared with the NCCIC. Such policies would only apply to DHS. Under the NCPAA, DHS' chief privacy officer would also be required to monitor implementation of privacy and civil liberties policies, and update privacy impact assessments on a regular basis to ensure privacy protections are followed.

Scope of Liability Protection

Each of the three bills provides liability protection for private entities that monitor their information systems for defensive purposes or share cyberthreat information with the federal government and/or with each other (depending on the sharing parameters of each bill). The bills state that a cause of action cannot be brought against a private entity for any actions taken that are authorized under the acts. However, the protections of the House bills will not apply in instances of "willful misconduct" (defined as an act or omission taken intentionally to achieve a wrongful purpose, knowingly without justification, and in disregard of risk of highly probable harm that outweighs any benefit).[6] CISA, in comparison, includes the "willful misconduct" exception, but also states that liability protection shall not apply in cases of "gross negligence." In addition, the House explicitly provides liability protection for a "failure to act" on cyberthreat data, a provision neither welcomed by the White House nor included in CISA.[7] Thus, any cause of action brought against a private entity for the sharing of cyberthreat information or use of defensive measures would be required to demonstrate willful misconduct.

The PCNA, NCPAA and CISA all explicitly state that nothing in the acts shall be construed to subject nonfederal entities to liability for choosing not to engage in the voluntary sharing of cyberthreat indicators or any other activity authorized by the act (such as employing defensive measures). Further, each bill states that the federal government cannot compel or coerce companies to participate, and cannot condition other benefits or contracts on participation.

CISA states that providing cyberthreat indicators or defensive measures to the federal government shall not constitute a waiver of any applicable privileges or protections provided by law, including trade secret protection. Additionally, the bill states that no provisions shall be interpreted so as to permit violations such as price-fixing, allocating a market among competitors, etc.[8] However, the mere sharing of cyberthreat indicators between two or more private entities would not be considered a violation of antitrust laws under CISA, echoing by statute a joint statement by the Department of Justice and the Federal Trade Commission.[9] The NCPAA also includes similar antitrust language.[10]

Other CISA Provisions

CISA includes a number of other provisions pertaining to cybersecurity that are not included in the House bills. These include a full title on bolstering federal network security and cyber defensive systems and a title on assessing the federal cybersecurity workforce and identifying roles of critical need. The House bill prohibits federal, state and local governments from using shared cyberthreat information to regulate businesses, while CISA suggests there may be some authority to regulate indirectly based on information shared by the private sector with the public sector.

Of particular concern to some in private industry is CISA Section 407, which would require the secretary of homeland security to submit reports to Congress on the extent to which entities identified as owners or operators of critical infrastructure report significant intrusions of information systems essential to the operation of critical infrastructure to DHS. Section 407 would then require DHS to develop, within 180 days, a strategy to mitigate the effects of any future intrusions such that they would no longer reasonably result in catastrophic regional or national effects.

CISA also contains a 10-year sunset provision from the date of enactment, in contrast to a seven-year sunset passed by the House, but would permit any actions authorized by the bill taken before the sunset to continue in effect as necessary.

Conference Committee Ahead

With passage in the Senate, CISA now moves to the final legislative phase — it will be conferenced with the two previously passed House cybersecurity bills. A conference committee schedule and conferees have yet to be agreed upon, and it is unclear at this time what path and timing may ultimately lead to the president's desk and passage into law. Despite the challenges facing the conferees, all three bills passed with strong support from both sides of the aisle, and generally from the White House, thus partisan issues are not likely to derail negotiations at this stage.

Looking much further down the road, although participation under the statute is voluntary, if cybersecurity information sharing becomes commonplace and is a highly effective and valuable tool, there may be pressure from various constituencies to participate. For example, it is possible that some companies may require their supply chain vendors to participate in some fashion. The impact of the legislation may be felt far and wide and companies of all types should be following these developments.

—By David Turetsky, Francine Friedman and Matthew Thomas, Akin Gump Strauss Hauer & Feld LLP

David Turetsky is a partner in Akin Gump's Washington, D.C., office and former chief of theFCC's Public Safety and Homeland Security Bureau. He co-heads the firm's cybersecurity, privacy and data protection practice.

Francine Friedman is senior policy counsel in the firm's Washington office and former senior vice president of Parven Pomper Strategies Inc.

Matthew Thomas is a senior public policy specialist at the firm.

[1] Remarks by President Obama at the Cybersecurity and Consumer Protection Summit, Stanford University, February 13, 2015

[2] Ibid.

[3] See generally, "Information Sharing Bill Includes Numerous Privacy Protection Provisions," Press Release from Senator Dianne Feinstein (D Cal), October 30, 2015. Some opponents, however, continue to argue that the bill insufficiently protects privacy and could aid surveillance. See "CISA Security Bill Passes Senate With Privacy Flaws Unfixed", Wired.com, October 27, 2015 available at http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/.

[4] See H.R. 1560 §§ 2 & 3, H.R. 1731 § 3, and S. 754 §§ 3-5.

[5] See S. 754, Section 104(d)(2).

[6] Willful misconduct may include knowingly sharing of personally identifiable information.

[7] See H.R. 1560, Protecting Cyber Networks Act, Section 106(b).

[8] See S. 754 § 8(e).

[9] See Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information, April 10, 2014.

[10] See H.R. 1731 § 3(4)(i)(10).