Public Policy | Privacy, Data Security & Information Use | November 10, 2015

Senate Passes Cybersecurity Information Sharing Bill Long Sought by Industry

By Brian E. Finch, Elizabeth Vella Moeller and Craig J. Saperstein

This alert also was published as a bylined article in the *Westlaw Journal Computer & Internet* on December 4, 2015.

On Tuesday, October 27, the U.S. Senate approved legislation, strongly supported by business groups, that would facilitate information sharing between government and industry and provide liability protection to companies that participate. The Cybersecurity Information Sharing Act of 2015 (CISA) passed the Senate by a bipartisan vote of 74-21, setting the stage for a House-Senate conference committee that will work to resolve differences between CISA and similar legislation passed by the House in April and to prepare a final bill to be considered by both chambers of Congress for potential enactment into law.

This client alert describes the major provisions of the bill, analyzes the bill's privacy protections, summarizes the amendments considered on the Senate floor, and forecasts the next steps needed to resolve differences between the Senate bill and similar bills passed by the House, as well as the remaining legislative hurdles that must be overcome for the provisions to become law.

Major Provisions of CISA

CISA establishes a voluntary system under which private entities and the government can share and receive technical information, including cyber threat indicators and defensive measures—in real time with each other via an automated process. This information about emerging threats and the response to those threats would be sent by an entity to a portal at the Department of Homeland Security (DHS). There, DHS would analyze the information and immediately share it with other participating entities across the country to help them defend against similar attacks. Additionally, the bill requires the government to share more of its own cybersecurity information than it has in the past, including classified information that is protected with proper safeguards.

In exchange for participation in the cybersecurity information sharing network, CISA provides private entities with significant legal liability protection. Without such protection, entities have been reluctant to share cyber threat information because of concerns about antitrust violations, regulatory actions, the potential misuse of intellectual property, the loss of trade secrets and proprietary business information, and suits from privacy advocates. CISA grants liability protection from any civil cause of action that is brought in relation to the monitoring of information systems or the sharing of cyber threat indicators that is conducted in accordance with the bill, except if an entity has engaged in gross negligence or willful misconduct.

The provisions of CISA would sunset after 10 years.

Privacy Considerations

Proponents of the bill, including Senate Select Committee on Intelligence (SSCI) Chair Richard Burr (R-NC) and Vice Chair Dianne Feinstein (D-CA), convinced their colleagues that the latest version of CISA can improve the country's cybersecurity while simultaneously protecting Americans' privacy. They point to safeguards in the bill that protect personal information by placing limits on the government's use of cyber threat information[1] and by authorizing the Attorney General and the Secretary of Homeland Security to implement privacy guidelines associated with the information-sharing system. Additionally, the bill requires the federal government to review cyber threat indicators to assess and remove anything known to be personal information or that identifies a specific person not directly related to a cybersecurity threat before sharing. The Obama Administration effectively endorsed CISA's privacy provisions by issuing a supportive Statement of Administration Policy on the bill.

Some technology companies, including Apple, as well as privacy advocates oppose the legislation, arguing that CISA fails to adequately protect users' privacy and creates the potential for corporations to share large amounts of an individual's personal information with the government. They have expressed concerns that the government could use the information not just for cybersecurity purposes, but also for federal law enforcement and National Security Agency surveillance.

Action on the Senate Floor

During Senate floor consideration of CISA, lawmakers debated a variety of amendments to the legislation, including several addressing the bill's perceived shortcomings with respect to privacy. Several of these amendments, viewed by industry stakeholders backing the legislation as "poison pills" that would have undermined the information-sharing regime to such an extent that they would have rescinded their support of the bill, failed in Senate floor votes. In particular, the Senate defeated several amendments to require more careful scrubbing of cyber threat indicators by both private entities and DHS to ensure the removal of personal information, as well as one amendment that would have protected personal information that is *reasonably believed* to be personal information, as opposed to the bill's current protection for information *known* to be personal information. The Senate also rejected an amendment that would have removed language exempting the information-sharing program from Freedom of Information Act requests.

[1] *See* S.754 §05(d)(5)(A), which states that cyber threat indicators and defensive measures can only be used for: "a cybersecurity purpose;" "identifying a cybersecurity threat;" "responding to or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm;" "responding to, or otherwise preventing, a serious threat to a minor, including sexual exploitation;" or "preventing, investigating, disrupting, or prosecuting" certain fraud, identity theft, espionage or trade secret provisions in the U.S. Code.

An amendment by Sen. Tom Cotton (R-AR) that would have expanded liability protection to cybersecurity information shared outside of the DHS portal with the Federal Bureau of Investigation (FBI) and the U.S. Secret Service also failed, despite strong support from several industry groups. Trade associations from certain infrastructure sectors—such as retail, restaurants, grocers, and convenience stores—advocated for the change because the FBI and the Secret Service are their primary contact points in fighting cyberattacks. While this provision was included in a similar bill passed by the House of Representatives, opponents of the amendment wanted to centralize incoming cyber threat indicators and were concerned about the capabilities of the FBI and the Secret Service to scrub the personal information from that shared information.

Although the Senate voted not to adopt a variety of amendments, it did approve a "manager's amendment," a substitute version of the bill prepared for Senate floor consideration which included largely non-controversial amendments and technical corrections to the version of the legislation passed by the SSCI. One provision in the manager's amendment, authored by Sen. Tom Carper (D-DE), would authorize the use of the nascent DHS cyber intrusion detection and prevention system—known as EINSTEIN 3A—across the federal government. This technology can analyze network traffic to identify and stop cyber threats. However, as of this July, less than half of federal personnel are currently using the EINSTEIN technology, in part because there is some legal uncertainty regarding the agencies' authority to participate.[2] The Carper amendment clarifies the legal foundation for expanding the use of this technology, mandates agency adoption, and requires DHS to improve the system's capabilities. The bill requires DHS to regularly assess the system through operational tests and evaluations in real world or simulated environments and permits the use of commercial technologies to improve the system. The bill also mandates that the DHS develop a pilot to acquire, test, and deploy, as rapidly as possible, the new technologies.[3]

Next Steps

The U.S. House of Representatives previously passed two similar bills on the topic of sharing cybersecurity information sharing: H.R. 1560, the Protecting Cyber Networks Act (PCNA), and H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (NCPAA). We expect the two chambers to work to resolve the differences between CISA, PCNA and NCPAA through a conference committee consisting of members of both chambers, from both parties. The conference committee members will largely consist of lawmakers from the House and Senate Intelligence Committees and the House Homeland Security Committee—all three of which played a role in developing the bills. The conference committee will aim to negotiate one final version of the bill, known as a conference report, that each chamber would then likely consider under a final "up or down" vote. To ensure that the President is willing to sign the bill into law, lawmakers may take into account the Obama Administration's positions with respect to information-sharing legislation, including its opposition to additional liability-protected sharing channels and its concerns regarding the types of defensive measures authorized under the information-sharing bills.

Agreement will need to be reached on several key differences between the information-sharing bills. For instance:

[2] *See* Statement by Secretary of Homeland Security Jeh Charles Johnson to the U. S. House of Representatives Committee on the Judiciary, July 14, 2015, p. 5.

[3] *See* S. 754 § 230(c)(4)-(5).

- The CISA includes liability protection from certain antitrust laws that the House-passed bills do not cover, and the PCNA includes protection for information shared with the FBI and Secret Service.

- The NCPAA specifically highlights the DHS National Cybersecurity and Communications Integration Center (NCCIC) as the lead federal civilian interface for information sharing, whereas PCNA and CISA require the Director of National Intelligence to develop appropriate procedures for the DHS portal.

- The House versions of the bill each contain a seven-year sunset, which is three years shorter than CISA's sunset provision.

- The House bills do not contain the language regarding the expansion of the EINSTEIN 3A program to protect federal networks.

- Finally, the bills have slightly different definitions of "cyber threat indicator" and "defensive measures"—including PCNA's definition of cyber threat indicators that includes physical objects that can be shared with the government.

Conference discussions are expected to occur later this year or early next year. Once a final bill is enacted into law, CISA calls for the Attorney General and Secretary of Homeland Security up to 180 days to finalize procedures for sharing cyber-threat information. Stakeholders will likely have the opportunity to comment on the implementation of the rule and will need to develop policies and procedures to comply with it.

(The authors would like to thank Chris K. Leuchten for his contribution to this publication.)

If you have any questions about the content of this alert please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Brian E. Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Elizabeth Vella Moeller (bio)
Washington, DC
+1.202.663.9231
elizabeth.moeller@pillsburylaw.com

Craig J. Saperstein (bio)
Washington, DC
+1.202.663.9244
craig.saperstein@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP
Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.