Advisory

OCTOBER 2015

If you have any questions about this Advisory, please contact:

DAVID HALL
215.988.8325
dhall@wiggin.com

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

U.S. Senate Moves Forward on Cybersecurity Information-Sharing Legislation

On October 27, 2015, the U.S. Senate passed the Cybersecurity Information Sharing Act of 2015 ("CISA") by a vote of 74-21. CISA had been stalled in the Senate since its submission in April 2015 by Senators Diane Feinstein (D-CA) and Richard Burr (R-NC), the Vice Chair and Chair, respectively, of the Senate Intelligence Committee. There is a strong belief within the business community that if current cyber-threats and data from previous attacks could be amalgamated, analyzed, and shared with other companies and the federal government, then broad spectrum defense strategies could be developed to protect American business as a whole. However, concerns about the bill's privacy protections from opposing senators, privacy and civil rights groups, and segments of the tech industry have contributed to extended inaction and negative press regarding the legislation.

The bill authorizes information sharing of "cyber-threat indicators" between private entities and the federal government, including system security vulnerabilities, methods of defeating system security, and patterns of communications that appear to target and exploit cybersecurity weaknesses. If passed, the bill calls for the Attorney General and Secretary of Homeland Security, in conjunction with heads of other federal agencies, to develop guidelines and standards for sharing cyber-threat information. The bill requires the federal government to share cyber-threat information with private companies but specifically does not require corporations to share information with one another or with the government. A sunset clause was also added to the bill during the recent floor debate, requiring that the legislation expire in 10 years unless reaffirmed.

The most important portion of the bill, the liability protections for companies that do choose to share cyber-threat information, remained intact after the vote despite a series of amendments from Senators Rand Paul (R-KY), Al Franken (D-MN), and Ron Wyden (D-OR) which would have diluted liability protections and placed additional duties on companies to remove personal data before sharing. The bill has been lambasted by privacy advocates and civil rights groups, including the ACLU and Electronic Frontier Foundation, as a domestic spying bill that will allow the federal government to compile private citizen data under the cover of cybersecurity concerns. The requirement that companies review and reasonably attempt to remove individual personal data prior to sharing information is still included in the bill, but companies do not lose the liability protections of the bill if they mistakenly share customer data.

There remain several bars to CISA's ultimate passage into law. First, CISA must be reconciled with a sister version of the bill in the House. The House version of the bill, known as the Protecting Cyber Networks Act ("PCNA") that was

CONTINUED ON NEXT PAGE

U.S. Senate Moves Forward on Cybersecurity Information-Sharing Legislation

passed in March 2015, contains several differences from CISA regarding liability protections, allocations of power to certain federal agencies to regulate and create guidelines for sharing, and the permissible uses of shared information by the federal government. All of these differences could be resolved in committee by the sponsors of the bills, but the acts each face strong opposition from privacy-driven members in both houses of Congress. Furthermore, opposed senators could opt to filibuster the bill if their demands regarding privacy and liability limitations are not accommodated. If a final version of one or both bills does manage to survive a vote in Congress, then passage is almost certain given the White House's endorsement of CISA and renewed calls for information sharing legislation in August 2015.

If CISA or the PCNA do become law, cyber-threat information sharing is likely still a long way off. CISA's present language allows the Attorney General and Secretary of Homeland Security to take up to 180 days to finalize guidelines and standards for information sharing. Most private industry is unlikely to begin sharing information before firm guidelines and liability protections are in place. Moreover, private companies' participation in information sharing will largely depend on the structure that liability protections take in the finalized version of the bill, as well the intensity of any public outcry over the bill's impact on individual privacy. The bill's ultimate usefulness, if it becomes law, will largely turn on whether the reconciliation of CISA and the PCNA will incentivize American businesses to share their cyber-threat information while providing assurances of privacy for the American public.

Stay tuned.

A special thank you to John Foley for his assistance in co-authoring this alert.