Advisory

FEBRUARY 2016

The Cybersecurity Act of 2015

On December 18, 2015, the President signed into law the Cybersecurity Act of 2015 ("the Act"). The intent of the Act is to encourage more interaction between the government and the private sector, as well as within the private sector, on the sharing of cybersecurity threat information.

One feature of the Act is to require the federal government to develop procedures for the dissemination of classified cyber threat indicators to non-government entities, as well as periodic sharing of cybersecurity best practices. Unanswered at this stage is the question of what useful classified information the government has been withholding, as well as the question of how the government will disseminate information if it is truly classified.

The Act authorizes the voluntary sharing and receipt of cyber threat indicators and defensive measures among governmental and private sector entities. The Act requires that businesses remove information that identifies specific individuals prior to sharing, and provides protections from disclosure of shared information under the Freedom of Information Act.

One of the major goals of the legislation is to provide liability protection for private entities that share cyber threat information. To this end, the Act provides that no cause of action shall lie or be maintained against a private entity for information-sharing of cyber threat indicators or defensive measures. An exception for gross misconduct that appeared in previous bills was deleted. In addition, the Act includes an antitrust exemption, designed to provide protection from potential antitrust violations for the sharing of cyber threat indicators. These protections, however, are not absolute and should be carefully evaluated before information is shared.

While the Act does provide an avenue for information-sharing – a long-sought-after tool for combatting cyber threats – it does not address several other important cybersecurity concerns. The Act does not, for example, provide for a uniform federal cyber reporting standard, leaving in place the mosaic of 47 different state standards. Similarly, the Act does nothing to create a uniform federal cybersecurity standard or safe harbor for private industry. Thus, the competing interests of a multitude of different federal regulators – including the FTC, the FCC, and the SEC – will remain unaligned.

Several groups, including the U.S. Chamber of Commerce and National Retail Federation, have hailed the passage of the Act as a victory and a strong first step towards improving national cybersecurity. However, the Act's critics are many and include a group of large Silicon Valley

CONTINUED ON NEXT PAGE

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

DAVID HALL
215.988.8325
dhall@wiggin.com

The Cybersecurity Act of 2015

tech-companies (Apple, Twitter, and Yelp) and the Computer & Communications Industry Association. Many tech-companies harbor significant concerns about the privacy implications of the Act and, as a result, say they will not engage in information sharing under the Act.

The Act is intended to provide a relatively risk-free environment for private industry to expand its cybersecurity knowledge base and to develop sustainable networks of information-sharing. Whether this approach will be effective in addressing cyber threats to customer data and intellectual property remains to be seen.

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