CARLTON FIELDS

New Federal Law Protects Companies that Share Cyber Threat Information

January 05, 2016

On December 18, the President signed into law as part of the federal omnibus government spending package a number of cybersecurity provisions, most notably the "Cybersecurity Information Sharing Act of 2015" (CISA). CISA provides incentives for cyber threat sharing with the federal government and among private industry by establishing liability protections for companies that monitor information systems or share or receive cyber threat indicators or defensive measures. Information sharing with the government and within industries has long been touted as a way to combat cyber threats. Businesses and other entities, however, have been wary of exposure to regulatory action and/or civil liability as a result of any such information sharing. Further, the private sector has been concerned with the waiver of applicable privileges and other protections if cyber threat information were shared with the government. The passage of CISA aims to address those concerns by (1) authorizing private entities to monitor their information systems and employ defensive measures to address cyber threats to those systems, and (2) authorizing private entities to share with one another and the federal government information regarding cyber threats and defensive measures undertaken in response to those threats. Further, CISA provides that no cause of action can be brought against private entities that conduct activities authorized by and in accordance with the Act. CISA ensures that applicable legal privileges and protections, such as trade secret protection, will not be waived by sharing information with the federal government. Additionally, the Act contains provisions exempting (1) shared information from disclosure under provisions of the Freedom of Information Act, and (2) participating private entities from antitrust laws. CISA also provides that cyber threat information shared with the federal government will not be used to regulate lawful activities and explicitly states that the Act should not be construed to create a private-sector duty to share cyber threat indicators or defensive measures or a duty to warn based on the receipt of such information. To take advantage of these protections, private entities must share cyber threat information in accordance with the Act, which will involve electronically sharing information with the Department of Homeland Security through a process yet to be established. Any personally identifiable information must also be removed from any information shared pursuant to CISA. Finally,

any defensive cybersecurity measures implemented must not involve hacking back or other offensive defenses that would destroy or substantially harm an information system or its stored data. CISA tasks various federal agencies with developing over the next several months additional guidance and processes to facilitate and promote cyber threat information sharing between and among the public and private sectors. Some of that guidance may attempt to address privacy and civil liberties concerns raised by critics of CISA. Accordingly, it will be important to monitor these developments subsequent to passage of the Act.

Authored By

Erin J. Hoyle

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology