wiley

ALERT

Senate Passes Cybersecurity Legislation in 74-21 Vote

October 29, 2015

On October 27, 2015, the U.S. Senate passed the Cybersecurity Information Sharing Act (CISA) by a margin of 74-21. The bill is designed to increase the ability of the private sector and federal government to detect and thwart cyberattacks in real time. In order to accomplish that, the bill directs the federal government to create procedures for the voluntary sharing of cyber threat indicators between the private sector and government. The bill envisions that the federal government will facilitate the ability to respond in real-time by creating a process that allows information sharing between federal entities "in an automated manner."

The bill provides protection for entities who share cyber threat indicators with the federal government, but only if the sharing is provided through a portal to be developed by the U.S. Department of Homeland Security. The bill requires dismissal of any claim based on the sharing or receipt of a cyber threat indicator or defensive measure, excluding claims based on gross negligence or willful conduct. In order to take advantage of the immunity offered in the bill, an entity would have to show that it complied with the procedures required by the bill, including procedures to protect the privacy of individuals. Specifically, before sharing a cyber threat indicator, an entity must take steps to remove any personal information or information that identifies a specific person not directly related to a cybersecurity threat that is known to the entity at the time when the cyber threat indicator containing such information is shared with the federal government.

The federal government can use the cyber threat indicators it receives in limited ways beyond just identifying and mitigating cybersecurity threats. For example, the federal government can use the information

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Public Policy

to investigate and prosecute certain imminent threats, including threats involving serious bodily harm, serious economic harm, terrorism, computer hacking, and the protection of trade secrets.

The bill also allows private entities to take a more active role in their own cyber defense. Under the proposed legislation, private entities may monitor their own information systems and engage in defensive measures for cybersecurity purposes. Although allowing defensive measures may provide a narrow exception to the Computer Fraud and Abuse Act, the bill does not allow for private entities to engage in full-scale cyberattacks on suspected hackers. Absent written consent, the defensive measures can only be applied to an entity's own information systems in order to protect the rights or property of the private entity.

Earlier this year, the U.S. House of Representatives passed two similar cyber threat sharing bills. The Senate bill will now go to conference with the House legislation to reconcile any differences and come up with a final bill. The Obama Administration has given conditional support to the bill.

If enacted, the bill presents an opportunity for private sector entities to improve their cybersecurity by quickly learning about active cyber threats. The challenge to companies will be to make proper decisions about when to share a cyber threat indicator with the government and what specific information should be shared. In particular, companies will have to take appropriate actions to make certain that they have complied with the requirements to remove known personally identifiable information from the cyber threat indicators both to qualify for immunity under the bill and to protect their users' privacy.