Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

OCTOBER 2015

# Cybersecurity Information Sharing Act Passes Senate, Would Encourage Business to Share Cyber-Threat Data with Government

Sharing information about cyber threats and analysis is a cybersecurity best practice but can often come into conflict with a company's protection of its own data and that of its customers. On October 27, 2015, the U.S. Senate passed the Cybersecurity Information Sharing Act of 2015 (S.754), or CISA, a law that would encourage private companies to voluntarily share information regarding cyber threats with other private entities and with the federal government. Under the bill, cyber threat information provided to the Department of Homeland Security would in turn be shared expeditiously with other federal agencies and with participating private entities. Backers of the legislation admit the law is but the first of necessary measures to better address the proliferation of cyber-attacks on businesses and governmental entities that have affected millions of Americans in recent years.

In furtherance of its purpose to encourage voluntarily sharing of information, CISA purports to provide considerable protections for companies that elect to participate in the program. Most notably, the bill provides broad immunity from suit related to companies' monitoring and sharing of cyber threat information. The bill also permits companies to share certain information without running afoul of antitrust laws; allows companies to retain legal privileges and protections with respect to shared information, including trade secret protection; and exempts shared information from certain public disclosure laws.

Although the bill passed the Senate by 74 to 21 and with the support of the U.S. Chamber of Commerce, it has received heavy criticism from privacy advocates, technology companies – like Apple and Dropbox – and industry trade groups. Opponents of the bill contend that it permits participating companies and the federal government to monitor and share customer data with inadequate restrictions and oversight, and does little to actually bolster the country's cyber defenses. The Senate has rejected, however, several proposed amendments to CISA that sought to address similar privacy concerns.

In response to these privacy-based objections, proponents of CISA have pointed to the bill's data protection provisions and bi-annual reporting requirements. For example, the bill requires that, before sharing cyber threat information, entities must remove irrelevant personally-identifiable information. The bill also enumerates the limited list of activities for which the federal government may disclose, retain, or use cyber threat information provided to it under CISA.

Before reaching the President's desk, the bill must be reconciled with two similar measures passed by the House of Representatives earlier this year.

To learn more, contact Clifford G. Tsan or Michael D. Billok (Co-Chairs of Bond's Cybersecurity and Data Privacy Group) or Brendan M. Sheehan.

| | | |
|---|---|---|
| Clifford G. Tsan | 315.218.8252 | ctsan@bsk.com |
| Michael D. Billok | 518.533.3236 | mbillok@bsk.com |
| Brendan M. Sheehan | 315.218.8276 | bsheehan@bsk.com |

BOND SCHOENECK & KING ATTORNEYS

*Commitment · Service · Value · Our Bond*