Authors

Robert L. Smith, II
rlsmith@Venable.com
202.344.4077

Janet C. Fisher
jfisher@Venable.com
202.441.5749

Dismas Locaria
dlocaria@Venable.com
202.344.8013

Andrew E. Bigart
aebigart@Venable.com
202.344.4323

House Intelligence Committee Announces Cybersecurity Legislation: Path Forward Uncertain

On November 30, 2011, U.S. Representative Mike Rogers (R-MI), Chairman of the House Intelligence Committee, and ranking member Dutch Ruppersberger (D-MD), introduced the Cyber Intelligence Sharing and Protection Act ("CISPA") to assist companies in sharing information with the government regarding cyber threats and attacks. On December 1, the Committee voted 17-1 to advance the bill (H.R. 3523).

The bill aims to help U.S. businesses protect themselves and their customers from domestic and foreign hackers looking to degrade, disrupt, or destroy systems or networks, and/or to steal corporate records, trade secrets, and other intellectual property. Specifically, the bill authorizes the government to share classified cyber threat intelligence with private sector entities that have an appropriate security clearance and where the sharing (1) is consistent with the need to protect U.S. national security and (2) is used by the private entity in a manner that protects the classified intelligence from unauthorized disclosure. The private sector, in turn, may use cybersecurity systems to collect cyber threat information and share such information with any other entity, including the government. Importantly, the bill provides that private entities are immune from civil or criminal liability for using cybersecurity systems or sharing information in accordance with the bill (or for not using such information).

The issue of U.S. cybersecurity, or the perceived lack thereof, has become an increasingly hot issue in Washington. On May 12, 2011, President Obama unveiled an International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, which set forth the Administration's view on managing global cybersecurity. Several cybersecurity bills have been introduced in the House and Senate, and Senate Majority Leader Harry Reid (D-NV) has vowed to "bring comprehensive cyber security legislation to the Senate floor for consideration during the first Senate work period of next year."

According to Chairman Rogers, "[t]here is an economic cyber war going on today against U.S. companies...There are two types of companies in this country, those who know they've been hacked, and those who don't know they've been hacked. Economic predators, including nation-states, are blatantly stealing business secrets and innovation from private companies."

Introduction of the bill follows recent reports that an Illinois water plant was the subject of the "first" foreign cyberattack against domestic infrastructure. (The Department of Homeland Security and the FBI have found no evidence that the damage was caused by a cyberattack.) Although the Illinois attack is now believed to have been a false alarm, there is a growing consensus among policy makers and the private sector that the U.S. is ill prepared for a cyberattack, particularly one that targets critical infrastructure or public works.

The bill appears to have broad support from both parties in Congress. In particular, according to Rep. Ruppersberger, "The bill maintains vital protections for privacy and civil liberties without any new federal spending, regulations or unfunded mandates." During markup, the Committee adopted two amendments by voice vote that added additional privacy protections to the bill.

The bill, which has been voted out of committee, could still change, as there are many moving parts and competing bills on the cybersecurity issue. In particular, Rep. Dan Lungren (R-CA) is working on a separate but similar bill regarding the federal government's role in working with critical private sector entities.

While it is difficult to surmise what provisions a final bill might include, Venable will continue to monitor legislative developments, as any bill that is ultimately signed into law will have a significant impact on a myriad of industries and companies, including data repository companies, data security companies, and government contractors.

If you have any questions about this alert or other cybersecurity matters, please contact one of the authors of this alert.
