THE NEW ENGLAND COUNCIL

Committee Update

May 4, 2012

House Addresses Series of Cyber-Security Bills

CISPA Passed

Last week, the House voted 248-168 to approve the controversial Cyber Information Sharing and Protection Act (CISPA). Some 140 Democrats and 28 Republicans voted against the bill (H.R. 3523), which would amend the National Security Act of 1947, which obviously did not contemplate the existence of cybercrime when enacted. CISPA would add provisions defining describing cyber threats as a "vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from either 'efforts to degrade, disrupt, or destroy such system or network'; or 'theft or misappropriation of private or government information, intellectual property, or personally identifiable information.'" CISPA would instruct the national intelligence director to develop voluntary guidelines for cyber threat information-sharing between industry and the federal government. The bill would also allow provisional security clearances in order to share classified intelligence with owners of critical networks to help them prepare against cyber attacks.

As the week unfolded, there was considerable pushback from privacy advocates regarding CISPA, and the day prior to consideration of the bill, the White House issued a strong veto threat saying, "H.R. 3523 fails to provide authorities to ensure that the nation's core critical infrastructure is protected while repealing important provisions of electronic surveillance law without instituting corresponding privacy, confidentiality, and civil liberties safeguards."

Bill sponsors Mike Rogers (R-MI) and C.A. “Dutch” Ruppersberger (D-MD) announced several changes to the original legislation on Tuesday in an effort to appease privacy advocates who had criticized the bill. An amendment from Congressman Robert Goodlatte (R-VA) to narrow the scope of permissible information to be collected and shared under the bill was approved by a vote of 414-1. Other changes include limits to how the collected information may be used, specification that no new authority would be given to federal agencies to use cyber security systems on private networks, and a provision to sunset the legislation after five years. Congressman Jim Langevin (D-RI) offered an amendment to extend the information-sharing provisions to critical infrastructure – including airports, public transit systems, and utilities – which may not be completely privately owned, but it was voted down.

In addition, the Obama Administration also criticized the lack of mandatory cyber security standards and broad liability protections offered to owners of critical cyber infrastructure, saying that they remove much of the incentive to implement strong cyber security protections. While the Senate's Cyber Security Act of 2012, sponsored by Senators Joe Lieberman (I-CT) and Susan Collins (R-ME), includes security requirements, Republicans in both chambers have been strongly opposed to a regulatory approach, preferring to rely on voluntary, industry-driven best practices and incentives. Co-Chairs Edward Markey (D-MA) and Joe Barton (R-TX) of the Bipartisan Congressional Privacy Caucus also criticized the measure for failing to provide explicit protections for individuals' privacy.

Most recently, White House "Cyber security Coordinator" Howard Schmidt appeared on CSPAN emphasizing the White House's objections to CISPA, specifically the privacy issues, suggesting the veto threat still stands.

Other Cyber Bills Passed in House

In addition to CISPA, The House also approved three additional cyber security bills last week. The Federal Information Security Amendments Act (H.R. 4257), which would require continuous monitoring of federal agency networks rather than the current intermittent monitoring, was approved last Thursday under suspension of the rules. On Friday, the House approved H.R. 2096, which would direct federal agencies under the Networking and Information Technology Research and Development (NITRD) program to develop a plan to guide federal cyber security research and development efforts. The bill also reauthorizes cyber security programs through the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST). H.R. 3834 passed by voice vote and would require NITRD agencies, along with the National Science and Technology Council, to create and manage a strategic research and development plan for networking and information technology, including the targeting of new areas of research.

The expected next step for all the House-passed bills would be consideration by the Senate, but none of the bills have been introduced in the other chamber. The Senate is also considering several high-profile cyber security bills of its own.