THE NEW ENGLAND COUNCIL

Committee Update

April 20, 2012

"Cyber Week" in the House of Representatives

The House has declared next week to be "Cyber Week," and will focus on passing cybersecurity legislation. While the flagship legislation is the information-sharing H.R. 3523, there are a variety of cybersecurity bills making their way through the House which could potentially see action next week, either on their own or incorporated into broader legislation. Here is a brief summary of the major cybersecurity proposals currently under consideration in the House:

H.R. 3523: Cyber Intelligence Sharing and Protection Act (CISPA)

The House Intelligence Committee approved this bill, sponsored by Committee Chairman Mike Rogers (R-MI), on December 1, 2011 by a vote of 17 to 1. CISPA's main focus is to increase information-sharing between the federal government and private owners of critical cyber infrastructure. Under the bill, certain classified information about cyberthreats would be shared with private businesses to help them secure their networks against possible attacks, and businesses would share a wider range of data with the government. Of all the bills likely to be considered during cyber week, H.R. 3523 faces the most vocal opposition, largely from privacy advocates. Opponents of the bill, including the American Civil Liberties Union and various online privacy groups, believe that the language defining a cybersecurity threat would permit abusive retaliations against non-threatening websites. The groups pushing back against CISPA largely overlap with those who objected to the SOPA/PIPA anti-online piracy bills, also on the grounds that overly broad language would allow for abuses. Supporters of H.R. 3523 counter that the bill allows for cyberthreat information-sharing only, not retaliation against websites. The White House's National Security Council released a statement on Tuesday, April 17 criticizing the bill for not doing enough to address "the nation's critical infrastructure cyber vulnerabilities."

In contrast, Senators Joe Lieberman (I-CT) and Susan Collins (R-ME) drafted their similar cybersecurity information-sharing bill (S. 2105) after consultation with civil liberties groups in order to address some of their concerns about privacy. The Lieberman-Collins bill would also give more oversight authority to the Department of Homeland Security (DHS) in ensuring that critical networks are protected. Senate Republicans criticized the bill for the regulatory burden placed on businesses, and Senator John McCain (R-AZ) released a counter-proposal (S. 2151) which would rely exclusively on incentives rather than regulation to encourage companies to employ cybersecurity measures and share information.

H.R. 4257: Federal Information Security Amendments Act (FISMA)

The House Oversight Committee approved this bill, sponsored by Chairman Issa (R-CA), by voice vote on Wednesday, April 18. The legislation would reauthorize the E-Government Act of 2002, which was

aimed at protecting government information systems. FISMA would require continuous rather than intermittent monitoring of networks as well as regular cyber threat assessments. Each agency would designate a “chief information security officer” to oversee the network changes necessary to meet the bill’s requirements, and the Office of Management and Budget (OMB) would have ultimate responsibility for ensuring compliance. The OMB would also be tasked with the creation of a “central federal information security incident center” to disseminate security threat information, analyze breaches, and coordinate with the National Institute of Standard and Technology (NIST) on any security incidents. The House is expected to take up Chairman Issa’s bill during Cyber Week.

H.R. 3674: Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act (PRECISE)

This bill, sponsored by Congressmen Dan Lungren (R-CA) and Jim Langevin (D-RI), was also approved on Wednesday by a 16-13 vote in the House Homeland Security Committee. Originally, some Democratic Committee members were concerned that the changes went too far in curtailing DHS authority in cybersecurity efforts, although all offered amendments to increase the agency’s oversight were rejected. However, the bill now includes a set of approved changes from Congressman Lungren in an attempt to make the language more palatable and likely to be considered in the House next week. Under the latest version of the bill, DHS would coordinate public and private efforts to secure federal information networks, but would only participate in the protection of privately-owned critical networks when requested by the owners. The legislation also designates DHS’ National Cybersecurity and Communications Integration Center (NCCIC) as the clearinghouse for shared information on potential threats to cybersecurity, with $12 million over three years to support the Center’s efforts. The Committee also adopted an amendment from Congressman Michael McCaul (R-TX) allowing DHS to use certain information collected by federal agencies during cybersecurity activities to assess and counter any threats to federal networks. In response to concerns about network users’ privacy, another adopted amendment from Congresswoman Janice Hahn (D-CA) directs the DHS privacy officer to compile reports on the impact of DHS cybersecurity activities on privacy to ensure they abide by “all relevant constitutional and legal protections.” While this bill is a priority for the Homeland Security Committee, it is not favored by House leadership and not expected see floor action during Cyber Week.

Other Proposals

Congressman Michael McCaul (R-TX) sponsored the Cybersecurity Enhancement Act (H.R. 2096), and it was approved by the Committee on Science, Space and Technology on October 31, 2011. H.R. 2096 seeks to promote federal research and development into defense against cyber threats, as well as the advancement of cybersecurity technical standards.

Similar to the Cybersecurity Enhancement Act, the Advancing America’s Networking and Information Technology Research and Development Act (H.R. 3834) would also support federal research and development. However, H.R. 3834 has a broader focus on general information technology advancements rather than focusing on countering threats to cybersecurity. The Committee on Science, Space and Technology approved this bill from Congressman Ralph Hall’s (R-TX) on March 22.

A draft bill from Congressman Robert Goodlatte (R-VA) to increase penalties for cybercrime which

might have come up for a vote next week has been stalled by a recent ruling by the 9th Circuit Court of Appeals. In the *United States v. Nosal* case, the court ruled that the Computer Fraud and Abuse Act (CFAA) does not apply to employees who access company computers in order to steal proprietary information. Congressman Goodlatte decided to re-examine the bill's language, which would have made changes to update the CFAA, before submitting it for consideration by the House Judiciary Committee.

Chairwoman Mary Bono Mack (R-CA) of the House Energy and Commerce Committee's Manufacturing and Trade Subcommittee introduced the SECURE IT Act (H.R. 4263) as a companion to the Senate Republican cybersecurity bill introduced by Senator McCain. The bill was referred to the House Judiciary, Armed Services, and Intelligence Committees in addition to Congresswoman Bono Mack's own subcommittee, but she has indicated that she is waiting on direction from House leadership before moving forward on subcommittee consideration.