SQUIRE PATTON BOGGS

CONGRESS MOVES FORWARD ON CRITICAL CYBERSECURITY LEGISLATION: US HOUSE OF REPRESENTATIVES PASSES TWO MAJOR BILLS, SETS STAGE FOR SENATE ACTION

April 24, 2015

This week, during what the House dubbed as "Cyber Week," the chamber passed two major pieces of cybersecurity legislation that seek to update and authorize voluntary information sharing platforms that allow the federal government and the private sector to share information about cyber threat indicators they are seeing on their networks. The passage of these bills is an important step forward in passing meaningful cybersecurity legislation that will serve as a means to better protect the nation's critical infrastructure.

Every day, companies around the world are seeing increasingly sophisticated cybersecurity attacks and are looking for ways to protect their networks and the privacy of their employees and customers. These information sharing bills will provide a mechanism for companies to use to share information with the federal government about the cyber threats they are experiencing, while also receiving information from the government that will help them to better identify, mitigate and respond to cyber threats on their networks. These bills will have a tremendous impact on the private sector's ability to protect their networks by facilitating more effective and efficient ways to share information about cyber threats with the federal government. Critical infrastructure sectors like banking/financial services, health, transportation, energy, water/wastewater, communications, chemicals, manufacturers, information technology and many others will benefit greatly from this effort.

While many expected countless amendments to be filed during the House Rules Committee process, ultimately 61 amendments were filed and only 16 were ruled in order. In quick succession, the House passed the House Intelligence Committee bill, H.R. 1560 "Protecting Cyber Networks Act," on April 22, 2015 by a 307-116 vote. Then on April 23, the House also passed the Homeland Security Committee's National Cybersecurity Protection Advancement Act (H.R. 1731) by a 355-63 vote.

H.R. 1560 focuses on cybersecurity information sharing activities between the private sector and the Intelligence Community, including the US Department of Defense (DOD) and the Director of National Intelligence. The bill provides for targeted liability protections for private sector entities that choose to share information with the federal government regarding cyber threats. In addition, it includes a section on privacy and civil liberties to specifically address concerns from privacy advocates and requires multiple scrubs of data prior to sharing to remove personally identifiable information as a means to protect consumers.

The House passed five amendments, including a manager's amendment to make technical changes, and would include language in the bill that would do the following:

- Sunset the bill in seven years;
- Direct the Small Business Administration (SBA) to provide assistance to small businesses;
- Direct the Inspector Generals from the Intelligence Community, US Department of Homeland Security (DHS), US Department of Justice (DOJ) and DOD to report on procedures actually used to protect the private information; and
- Direct the Government Accountability Office (GAO) to assess the actions of the federal government to protection privacy.

H.R. 1731 authorizes the information sharing activities with the private sector and DHS, a civilian agency. It also includes liability protections for companies that share information with the federal government, which prompted several amendments to be proposed to scale back the liability protections in the bill. The House Rules Committee did not approve the consideration of these amendments but did allow 11 amendments to be debated on the House floor. The House passed all 11 amendments which would do the following:

- Sunset the bill in seven years;
- Codify the establishment of the National Cybersecurity Preparedness Consortium made of universities and other stakeholders;
- Provide cyber self-assessment tools for small and medium-sized businesses;
- Direct the GAO to assess the impact of the bill on privacy and civil liberties;
- Require a report to Congress on aligning federally funded cyber research with the private sector;
- Require a report from DHS on the assessment of cybersecurity at risk ports;
- Clarify the term "cybersecurity risk" and "cyber incident"; and
- Authorize the existing Einstein 3A (E3A) program.

The White House issued a Statement of Administration Policy (SAP) for each bill, noting that it supports the House's efforts to pass information sharing legislation. The SAPs did raise serious concerns by the White House over the current liability protection language. Specifically, the SAPs on both bills noted the White House's concern that "the use of defensive measures without appropriate safeguards raise significant legal, policy and diplomatic concerns and can have a deleterious impact on information systems and undermine cybersecurity." The SAPs also reiterated the need for incorporating privacy and civil liberties safeguards. However, the SAPs stopped shy of indicating if the changes were not made, the President may consider vetoing the bills.

Next Steps

The next steps for the bills are critical to note in order to understand how the process for moving information sharing legislation forward will unfold. While the House chose not to combine these bills prior to floor passage to have one comprehensive bill, it plans to combine the bills after final passage. From there, they will be sent over to the Senate for consideration.

The Senate Intelligence Committee previously passed its own information sharing legislation – the Cybersecurity Information Sharing Act (S. 754) – and is likely to move forward with considering the bill on the Senate floor in the next couple of weeks. Congressional leaders have indicated that they would like to have a final information sharing bill sent to President Obama by the Memorial Day recess, however the timeline is tight to achieve that goal.

An important part of this process will also be a determination in the Senate if they will allow comprehensive data breach bills to be added to its cybersecurity bill, which could potentially set up a complete overall to the nation's competing state data breach laws.

Contacts

Norma M. Krayem
Global Co-Chair, Data Protection and Cybersecurity
Washington DC
T +1 202 457 5206
E norma.krayem@squirepb.com

Amy Davenport
Washington DC
T +1 202 457 6528
E amy.davenport@squirepb.com