SQUIRE PATTON BOGGS

THE CONGRESS RAMPS UP ACTION ON CYBERSECURITY LEGISLATION

Possibilities For Data Protection/Breach Legislation Still Exist

While not a day goes by without a new cybersecurity attack, the recent news of the Russian criminal gang who is alleged to have stolen over 1 billion user names and passwords as well as 500 million email addresses reinforces the great need for action on cybersecurity legislation. In the face of continuing concerns over cybersecurity, both the House and Senate have moved quickly in just the last 30 days alone to move legislation forward.

It is clear that the recent activity in the House and Senate shows a commitment to moving individual cybersecurity bills forward which ultimately still have a chance for enactment this year. The "Lame Duck Congress" may well be the place for both cybersecurity and data protection/data security legislation to be completed.

The House passed four cybersecurity bills on July 28, 2014. These four bills included:

- The National Cybersecurity and Critical Infrastructure Protection Act (H.R. 3696) – This bill codifies and strengthens the current cybersecurity roles of the U.S. Department of Homeland Security (DHS) and focuses on actions to assist and work collaboratively with the private sector.
- The Critical Infrastructure Research and Development Advancement Act (H.R. 2952) – H.R. 2952 requires DHS to develop a strategic plan to guide the overall direction of federal cybersecurity research and development.
- The Homeland Security Cybersecurity Boots-on-the-Ground Act (H.R. 3107) – This bill directs the Secretary of Homeland Security to develop a workforce strategy to hire, train, recruit and retain a skilled DHS cybersecurity workforce.
- The Safe and Secure Federal Websites Act of 2014 (H.R. 3635) – H.R. 3635 prohibits any federal government agency from making any new websites that require personally identifiable information until the agency submits a certification to Congress that the website is fully functional and secure.

There has also been a flurry of activity in the Senate in the last 30 days as well, with some of the relevant Committees moving forward quickly to pass their respective bills out of Committee. There are several areas of cybersecurity policy that Congress is working on that we may see action on in the coming months. These areas include:

Federal Information Security Amendments Act (FISMA)

The Senate and House are currently considering bills to strengthen controls over Federal information and information systems in the .gov space, as well as to promote data sharing on cybersecurity issues like vulnerabilities and incidents.

Both chambers are working to update information management system guidelines across the Federal government. The Senate passed S. 2521, the Federal Information Security Modernization Act of 2014, out of the Senate Homeland Security and Governmental Affairs Committee without amendment on June 25, 2014. The House previously passed its version of the bill in April 2013. The bills are similar in many ways as both provide strong oversight and management of agency policies, procedures, and practices to protect Federal information and information systems.

However, the two versions differ in several key ways:

- For example, the House version would assign oversight to the Director of the Office of Management and Budget (OMB), while the Senate version would split these responsibilities with the Secretary of Homeland Security.
- The Senate version would also update how the Federal government responds to data breaches, including by requiring timely notice to those impacted. The House version does not contain any comparable provisions. If the Senate bill is passed, the two chambers will need to address these and other significant differences in conference.

National Cybersecurity and Communications Integration Center Act

As noted above, the House recently passed H.R. 3696 which has brought attention to the importance of codifying the existing DHS cyber roles and responsibilities. The Senate Homeland Security and Government Affairs Committee has also been working on a separate bill – the National Cybersecurity and Communications Integration Center Act (S. 2519) – that would codify the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC is an existing center within the Department of Homeland Security aimed at promoting information sharing among and between different levels of government and the private sector on cybersecurity matters. The Committee moved forward and successfully passed S. 2519 out of Committee at the end of June with minor amendments. H.R. 3696 focuses on a broader scope of DHS cyber roles than S. 2519, but the focus on codifying the NCCIC in both bills points to the importance of this center for cybersecurity information sharing.

Cybersecurity Information Sharing Bill and Privacy Concerns

The Senate Intelligence Committee, led by Chairman Dianne Feinstein (D-CA) and Vice Chairman Saxby Chambliss (R-GA), drafted the Cybersecurity Information Sharing Act (S. 2588), which was considered by the Committee in closed session on July 8, 2014 and passed by the Committee with three Senators opposing the bill.

- The bill focuses on incentivizing threat information sharing by the private sector, both among these entities and with the government.
- The bill would also authorize and provide liability protections for private companies monitoring information systems in accordance with the law.
- Privacy concerns continue with 22 groups sending a letter opposing the bill and raising serious concerns around efforts to protect personally identifiable information (PII), potentially overly broad liability protections and the "militarization" of the civilian cybersecurity programs.

The House companion bill, H.R. 624, the Cyber Intelligence Sharing and Protection Act, passed the House on April 18, 2013, but faces a threat of a White House veto due to concerns over PII as well.

Contacts

Norma M. Krayem
T +1 202 457 5206
E norma.krayem@squirepb.com

Ludmilla L. Savelieff
T +1 202 457 5125
E ludmilla.savelieff@squirepb.com

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

Samantha A. Martin
T +1 202 457 6314
E samantha.martin@squirepb.com

14442/08/14