Cooley

December 16, 2014

After years of pundits saying "oh, major cyber legislation will pass this year," it may finally be happening. Last week Congress hammered out details on four different cyber bills that are intended to help the country move forward with its cyber efforts. Ranging from information sharing, to workforce enhancement, to government cyber reorganization, the four bills represent arguably one of the most productive Congressional sessions in dealing with cyber issues (at least when measured by the sheer number of bills that have passed both the House and Senate). Only one of the bills, however, directly involves the private sector. The other three all focus on government cyber issues.

National Cybersecurity Protection Act of 2014

The most significant of the four bills (at least from a private sector perspective), the National Cybersecurity Protection Act of 2014 (S.2519), has been hailed by The National Law Journal as "The Most Significant Cyber Bill to Pass Congress in Over a Decade." The passage last Wednesday (December 10) of S.2519 formally codifies the National Cybersecurity and Communications Integration Center (NCCIC) within the Department of Homeland Security. The NCCIC provides a mechanism by which government, private industry, and other related stakeholders can share cyberthreat information. In particular, the NCCIC seeks to provide "shared situational awareness to enable real-time, integrated, and operational actions across [Government and commercial] entities to address cybersecurity risks and incidents." According to the NCCIC website, this shared situational awareness will be fostered by:

- proactive coordination of both cyber and telecommunications threats
- a "whole-of-nation" integration effort through engagement of a variety of partners
- breaking down barriers that impede useful collaboration
- serving stakeholders by being able to respond immediately and serve as a center of excellence

while at the same time "protect[ing] the privacy and constitutional rights of the American people."

Going back at least as far as the Commission on Cybersecurity for the 44th Presidency (2008), followed by the Coordinated National Cybersecurity Initiative (CNCI), information sharing between the public and private sectors has been identified as a necessary tool for fighting cybercrime. Given (a) the increasing skills and capabilities of the multitude of adversaries and (b) liability concerns over sharing information with either the government or other corporate entities, however, the sharing of cyberthreat information has been an elusive goal to achieve. The National Cybersecurity Protection Act seems to be a step in the right direction.

Although passage of S.2519 does represent a significant development regarding cybersecurity legislation, two things remain noticeably absent. First, the bill does not address the issue of anonymization. Stakeholders are often reluctant to share cyberthreat information for fear that doing so will expose weaknesses (or, worse, breaches) in their environment to the general public. A lack of anonymity reinforces this reluctance. In contrast to these concerns, the success of the Financial Services Information Sharing and Analysis Center (FS-ISAC) can be traced, at least in part, to the use of a Nondisclosure Agreement and a vigilantly enforced process for anonymous submission of cyberthreat information.

A second thing not addressed in the National Cybersecurity Protection Act is liability protection. Again, a fear of reprisal by either consumers or by business partners has often caused companies or other participants to not share cyberthreat information. The fear of a class action lawsuit or a lost contract can often outweigh the good that could result from the sharing of information that might help others in the ecosystem.

Neither of these issues, however, has a simple answer. Implementation of an anonymization approach requires a combination of technical and process deployments that must be properly coordinated in order for cyberthreat information sharing to successfully occur. If potential participants cannot be assured that shared information won't be attributed to them, they will be hesitant (at best) or completely disinterested (at worst) in participating. Thus, the NCCIC should investigate an anonymization approach. Similarly, detailed assurances about liability exposure might be needed for stakeholders to become comfortable with the NCCIC. At a minimum, a fear of

anti-trust accusations should no longer be a concern following the announcement in April by DOJ and the FTC that sharing of information security and cyberthreat information would not constitute grounds for an anti-trust action.

The other three

The remaining three bills passed by Congress all focus on the government and its obligations. The first, the Federal Information Security Modernization Act of 2014 (S.2521) contains amendments to the Federal Information Security Management Act (FISMA) that make the Department of Homeland Security (DHS) the central point of cybersecurity management and implementation for the federal government, while maintaining the existing authority of the Office of Management and Budget (OMB) over the information security policies of civilian agencies.

The remaining two bills that focus on cybersecurity within the government both involve the nation's cybersecurity workforce. The first contains portions the DHS Cybersecurity Workforce Recruitment and Retention Act (S.1691), which aims to improve both the hiring process and compensation for DHS employees that occupy cybersecurity positions. At least part of the goal is to retain federal cybersecurity workers working for DHS by creating parity between their pay and that of the Department of Defense (DoD). The second, the Cybersecurity Workforce Assessment Act (H.R. 2952), would require DHS to assess its cybersecurity workforce on a three-year basis. This assessment would complement the strategy for recruiting and training of that workforce.

Status

Both S. 2519 and S. 2521 passed the Senate on December 10, 2014, and await President Obama's signature. Similarly, S.1691 and HR. 2952 passed the House on December 11, 2014, having previously been passed by the Senate. This brings the number of cybersecurity bills now awaiting the president's signature to four.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140