There Oughta Be A Law (Well, Maybe)

This article was originally published on *FoxBusiness.com* on July 30, 2014.

by Brian E. Finch

Brian E. Finch
Public Practices
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian E. Finch is a partner in Pillsbury's Washington, DC office. His practice focuses on counseling on regulatory and government affairs issues involving the Department of Homeland Security, Congress, the Department of Defense, and other federal agencies.

This may come as a surprise to some people, but Congress is a legislative body designed to craft, debate and pass bills.

Seriously. That's what it says in the Constitution. I swear I once read it in there.

At the same time, Congress was also created to, well, not pass laws. Just because someone took the time to write a piece of legislation and introduce it in the House or the Senate it doesn't automatically follow that said legislation should become a law. Sometimes the law is duplicative. Other times it would not provide the timely solution to the problem it intends.

And then, of course, there are times when the legislation, well, just plain stinks. The Founding Fathers didn't explicitly talk about terrible legislation, but they certainly created a government structure that made it difficult to pass legislation. After all, a nation buried under laws, either good or bad, can quickly become an unworkable mess.

Stepping down from my constitutional law soapbox, the obvious question is: what does this have to do with cybersecurity?

Plenty, actually.

At any given time, there are dozens of pending pieces of legislation sitting at various stages of the Congressional sausage-making process. Some are relatively innocuous, dealing with issues such as workforce management or encouraging more research and development within the federal government. Other bills are intended to have a much deeper impact, imposing cyber regulations on portions of our economy.

Currently sitting in Congress are some good pieces of cybersecurity legislation. Others ... well, not so much.

To help those of you keeping track at home, I will highlight for you some of the better ideas floating around Congress. Some of these are in standalone bills, while others are tucked into larger bills. What they share in common, however, is that they represent forward-thinking legislating, and are designed to help the nation combat pressing cyber threats without resorting to heavy-handed regulation or unnecessarily duplicative efforts.

Of course, these are my thoughts and mine alone—and as family members often tell me, I am dangerous when I make my own decisions. Still, here goes nothing ...

- **Defense authorization bills**: Every year Congress passes a bill dictating what the military can do, including what it can spend money on. The National Defense Authorization Act is the primary vehicle through which Congress influences defense policy. It is no wonder that the bill runs hundreds of pages and addresses the minutia of various programs.

A careful read of the bill reveals some excellent ideas that deserve to be implanted. For instance, versions of the bill call for additional funding of various programs intended to detect and block so-called "zero day" attacks. Zero day attacks use previously unseen malware to attack heretofore undiscovered software and hardware attacks. In other words, zero days are stealthy attacks designed to hit weaknesses no one knew about except the bad guys. Obviously, blocking such attacks are critical, and so Congress gets it right by applauding programs intended to counter such attacks and encourage their wider deployment.

Other sections of the bill call for a more unified strategy to carry out cyber offense and defense, improving cyber "situational awareness," and bulking up the personnel structure of the military so that cyber skills are correctly valued and supported. Interestingly—and rightly, I believe—the bill also calls out for more clarity on weaknesses facing the Defense Department. For instance, the bill calls for an assessment of weaknesses in the logistics chain of the military.

Clearly, our adversaries have figured this out, as they are dedicating increasing resources to conduct sophisticated attacks on transportation and other support services. Napoleon once said, "An army marches on its stomach." And that holds true today—if our soldiers, sailors, and aircrews don't have food, fuel, and other critical supplies to fight their battles, well, the results will not be pretty. Thus Congress is right to protect that vulnerable supply chain.

- **Getting the Federal Cyber House In Order:** When it comes to criticizing the private sector for its state of cyber preparedness, the federal government is quite good at throwing stones. Well, someone should point out that the federal house is made of glass. The federal government suffers an enormous amount of cyber attacks on a daily basis. That in and of itself is not bad, much less unexpected. What is unacceptable, however, is how many of these attacks succeed, often due to lax or inadequate security procedures/technologies. Stories abound regarding outdated technology guarding vital networks, funding being directed to the wrong solutions, and, on occasion, the government failing to properly assign security responsibilities.

Such basic organizational structures are sadly common, but at least Congress is trying to do something about it. Updates are pending to the Federal Information Security Modernization Act, which governs how the federal government polices its own cyber networks. That law, as originally drafted, required periodic reviews and reports on cyber vulnerabilities and measures taken to remedy them. Well, we now live in a world of 24/7/365 cyberattacks, and the feds need to have their guard up constantly. The proposed legislation would go a long way to doing that, namely by calling for continuous monitoring of networks rather than scattered reports. The bill would also clearly define and divide the roles of the Department of Homeland Security and the Office of Management and Budget. A clear chain of command, especially when it comes to cyber defense, is always a good thing. That is particularly true when, as in this case, the clearly defined roles allow for federal agencies to better categorize cyber risks and thus work to address them in a rapid fashion. To me this is another "must pass."

- **Getting a Better Grip On The Role of DHS:** Eleven plus years after its inception, DHS is still trying to gain its sea legs. That's not a surprise, as no one expected the largest civilian reorganization of government in modern history to be an easy task. Still, the department sails a difficult course, as it has to be prepared to counter any hazard at any time.

Fortunately, there is good legislation moving through Congress that will help the Department of Homeland Security with its efforts. For instance, there is the National Cybersecurity and Critical Infrastructure Protection Act (NCCIP), which will soon be up for vote in the House of Representatives. This bill takes many good actions, including codifying and strengthening the National Cybersecurity and Communications Integration Center (NCCIC), a federal civilian, transparent interface to facilitate real-time cyber threat information sharing across critical infrastructure sectors. The bill

continues to grow public/private partnerships in a way that lends government resources without interfering with successful private sector security programs. The bill also provides some key incentives for investment in cybersecurity technologies and services, including limited liability protections where appropriate. The NCCIP is a perfect example of how some simple clarity with respect to roles and authorities can go a long way to providing a better, more coordinated response to cyber events.

Ultimately, the point I want to make is that not every Congressional bill with the word "cyber" in it is a "must pass." Instead, careful analysis is needed to determine whether the bill will actually help defend the country from digital threats. Most importantly, we have to resist the urge to reflexively support legislation that simply allows the government to "do more." A better plan is to support legislation that focuses the government on the "right thing" to do.

Now let's just hope the good people on Capitol Hill choose wisely.

Pillsbury Winthrop Shaw Pittman LLP