The Admiral Sets a Good Course

This article was originally published on *The Huffington Post* on June 20, 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.

Admiral Mike Rogers, the new leader of the National Security Agency and Cyber Command at the Defense Department, certainly has taken a different approach from his predecessor, General Keith Alexander. Right out of the gate, Admiral Rogers noted that the NSA had a public image issue and that it had lost some of its credibility with the American public.

That fresh take was welcomed by many. While continuing to tackle those issues, Admiral Rogers has also stuck to some existing themes, namely that American businesses need to step up and do more to protect themselves from cyber attacks. The comments by Admiral Rogers come as hopes for any legislative solution to cyber security are effectively disappearing this Congress. Election season, leadership changes, and a host of competing demands have made it fairly clear that - barring some disastrous event - another year will go by without Congress passing a law to address private sector cyber security.

So far so good in my book. Admiral Rogers does need to repair the NSA's image, and do a better job of explaining just what its mission is and why it has been so aggressive in collecting data. I also believe he is correct in urging private companies to do more to protect themselves from cyber attacks. That trend is already on the upswing, and further encouragement and support from Admiral Rogers will be key in those efforts.

I would add, however, that Admiral Rogers and the Obama Administration as a whole need to do more to explain what government's role is protecting against cyber attacks. I am not talking about how government could regulate the cyber security measures of companies or incentives it could offer to encourage more robust cyber defenses. No, here I am talking about what the government can and will do when it detects an attack being conducted by a foreign government.

Think of it this way: If an enemy army or air fleet is clearly on its way to attack targets in the United States, the military has a plan to respond. It has assets deployed domestically and overseas to intercept such attacks, and has tactics and strategies in place to respond to such aggressive maneuvers.

The same needs to be happening in the cyber attack domain. It is well known that foreign countries routinely penetrate private companies, sometimes for economic gain and others times for potentially more nefarious purposes. In many

ways I view this as no different from bombers flying a sortie against an American target. The owner of that target is not and should not be responsible for intercepting the bombers -- that is the job of the U.S. military. Plain and simple.

Establishing a doctrine and strategy to combat malicious cyber attacks will not be easy or cheap. But, it is something that has to be done, and someone like Admiral Rogers needs to step up and further develop such plans. They also need to be publicized, at least in a general fashion, as such plans will as much be about deterrence as anything else.

So I applaud Admiral Rogers for setting the NSA and Cyber Command on a new, better, course. More way points need to be added, however, for it to truly match American security needs.