5 Questions for the New Defense Secretary

This article was originally published on Fox Business on December 2, 2014.

by Brian E. Finch

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

Brian E. Finch is a partner in Pillsbury's Public Policy practice in Washington, DC. He is a recognized authority on global security matters and is co-leader of the firm's Global Security practice.

"Revolving door" is a favorite pejorative term associated with the Washington job market. It refers to the cycle of lawyers, lobbyists, and policymakers that leap between private sector jobs and mid to high-level bureaucratic or legislative spots. Many, such as the President, decry this "plague" as creating a culture of coziness that devalues the interests of Joe Taxpayer.

The revolving door analogy can also refer to the dizzying spin felt by some government employees as they are quickly spun out of a job. And yes, I'm referring to the soon-to-be former Secretary of Defense, Chuck Hagel.

As a replacement is chosen for Secretary Hagel, some important questions should be asked of the nominee at his or her Senate confirmation hearing.

Even knowing that the Senate Armed Services Committee is quite adept at conducting cybersecurity oversight, I offer up five cyber security questions to be asked:

1. **What will be your strategy for the offensive use of cyber weapons?**

   This is a biggie. It took a significant amount of time and effort just to determine whether cyber weapons should be treated like any other weapon under the laws of war (I should know, I wrote a paper about it in law school in the 1990s, don't ask me what grade I received).

   The rules of engagement with respect to the offensive use of cyber weapons have remained somewhat murky, many argue deliberately so. Still, I think this is a question that deserves a clearer answer and some publicity around relevant details.

   Our enemies seem to have no problem using cyber weapons offensively, and so I think it only prudent for us to set forth a strategy of when such weapons could be used. I don't need to know how, but I do think it is fair to say, "Here are our thoughts on using cyber weapons, everything is on the table except (directly harming civilians, etc.)."

2. **Do you support NSA and Cyber Command having the same senior officer?**

   Right now we have the same person running the National Security Agency (responsible for intelligence gathering, including by cyber means) and Cyber Command (responsible for defensive and offensive operations). Is it wise to have the military's chief spymaster also be in charge of defending and weaponizing cyber space?

   I don't really have an answer for this one, but I do think it is a

debate worth having. Especially in the post-Snowden era, we owe it to ourselves to examine this issue. The blunt reality is that most Americans, and foreigners for that matter, don't trust the NSA. They view it as a giant vacuum, sucking in every bit of data possible without regard for privacy rights. And then you have the same person running the NSA also in charge of the militaryís overall cyber operations. You can see how from a public relations perspective alone that creates a problem, and that's without asking legitimate questions about whether one person can adequately handle both tasks.

Take good notes on that answer, I'm curious what the nominee will have to say.

3. **What are your plans for modernizing cyber defenses amongst the various services?**

The Defense Department certainly has plenty of advanced widgets at its disposal. At the same time, their dissemination throughout the service branches is spotty at best.

We cannot afford to have any part of the military relying on last generation technology, especially in a threat environment where our enemies are so skilled in finding new exploits. Practically speaking, that means ensuring that non-signature-based defenses, data loss prevention tools, mobile security systems, and cybersecurity baked into technology DNA are all obligatory purchases.

And these defenses have to be quickly rolled out everywhere. The Manning saga is the only lesson we need to show that when some place is "last" or considered a low priority for security tool deployment, then that is where the breach will occur. The nominee's strategy for doing so is vital information as far as I am concerned.

4. **Will you continue the policy of laying blame for cyber breaches at the feet of vendors?**

Oddly, we live in a world where defense contractors tend to take the blame when they suffer a cyberattack. Take for instance the comments of the F-35 fighter program leader on the rash of malware found in the planes. The general felt confident that the Defense Department's security measures were not to blame, but rather it was the contractor's fault, noting *"I'm a little less confident about industry partners to be quite honest with you ... I would tell you I'm not that confident outside the department"*.

Hmm, bold statements from a group that failed to assign responsibility for cybersecurity in a project, leading to a major breach by Iranians. Or the Department that suffered the most damaging cyberattack in American history thanks to Edward Snowden.

Would it be acceptable to place blame on Lockheed Martin if the Chinese bombed an F-35 manufacturing plant? Of course not, and we should not automatically lay blame at the feet of government contractors when foreign nations lay siege to their electronic systems. The Defense Department is doing the right thing by requiring contractors to implement more security, but we also have to realize at a certain point they cannot protect themselves.

We should hear from the nominee on how the Defense Department plans to hold itself, and not just vendors, accountable when it comes to cyberattacks.

5. **How will you ensure that cybersecurity is a real priority and not just a budget tactic?**

Every cabinet agency seems to be using cybersecurity to justify new purchases or assertions of authority. However, we want to ensure smarter spending on cybersecurity, not just throw dollars at the problem.

Money has to be spent the right way, and in my world that means two key things: a balance between security and incident response, and avoiding the "Lowest Price Technically Acceptable" trap.

First, even the Defense Department admits that it has to learn to "live with the adversary on the system." Translation? Successful attacks will happen, and at some point an unauthorized user will be in its network. That said, money has to be spent wisely on finding and removing intruders, not just from keeping them outside the walls of the fort.

Second, the Defense Department, like every agency, is facing budget pressures. It is responding in part by using the "Lowest Price Technically Acceptable" procurement model, under which the cheapest priced product will be purchased assuming it meets bare minimum standards. That's not a good model. Instead we need to use the "Best Value" model, which helps ensure that the

product has all the right pieces, even if it is a little more expensive.

Thus, how the nominee will engage in "smart" cyber procurements is yet another critical question worth exploring.

The next Defense Secretary nominee will face these and many other questions at the confirmation hearing. I would not want to be in his or her shoes given the current budget and threat environment.

Still, when it comes to cyber, this is going to be as good a time as any to ask some hard questions that deserve solid answers.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | +1.877.323.4171

Pillsbury Winthrop Shaw Pittman LLP