SENATOR JOHN MCCAIN
OPENING STATEMENT
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
HEARING: CYBERSECURITY ACT of 2012
FEBRUARY 16, 2012

Mr. Chairman and Ranking Member, thank you for holding this hearing on the long awaited 'Cybersecurity Act of 2012.' I welcome our panel, and specifically, Senators Rockefeller and Feinstein, Secretary Napolitano, and Governor Ridge and thank everyone for the willingness to share their perspective.

I would like to state from the outset that I have sincere fondness and respect for the Chairman and Ranking Member – especially when it comes to matters of national security. So, whatever criticisms I may have with the legislation, should not be interpreted as an attack on the lead sponsors, but rather on the process by which the bill is being debated and it's policy implications.

All of us recognize the importance of cybersecurity in the digital world. Time and again, we have heard from experts about the importance of possessing the ability to effectively prevent and respond to cyber threats. We have listened to accounts of cyber espionage originating in countries like China; organized cyber criminals in Russia; and rogue outfits with a domestic presence like 'Anonymous,' who unleash cyber-attacks on those who dare to politically disagree. Our own Government Accountablity Office has reported that over the last five years, cyber-attacks against the United States are up 650 percent. The threat is real.

It is my opinion that Congress should be able to address this issue with legislation a clear majority of us can support. However, we should begin with a transparent process which allows lawmakers, and the American public to let their views be known. Unfortunately, the bill introduced by the Chairman and Ranking Member has already been placed on the calendar by the Majority Leader, without a

single markup or any executive business meeting by any committee of relevant jurisdiction. My friends, this is wrong.

To suggest that this bill should move directly to the Senate Floor because it has "been around" since 2009 is outrageous. First, the bill was introduced two days ago. Secondly, where do Senate Rules state that a bill's progress in a previous congress can supplant the necessary work on that bill in the present one? Additionally, in 2009 we were in the 111th Congress with a different set of Senators. For example, the minority of this Committee has four Senators who were not even in the Senate, much less on this Committee, in 2009. How can we seriously call it a HSGAC product without their participation in committee executive business? Respectfully, to treat the last Congress as a legislative mulligan by bypassing the committee process and bringing the legislation directly to the floor is not the appropriate way to begin consideration of an issue as complicated as cybersecurity.

In addition to these valid process concerns, I also have policy issues with the bill.

A few months ago, the Chairman of this Committee and I introduced an amendment to the Defense Authorization bill codifying an existing cybersecurity Memorandum of Agreement (MOA) between the Department of Defense and the Department of Homeland Security (DHS). The purpose of that amendment was to ensure that this relationship endures and highlight that the best government-wide cybersecurity approach is one where DHS leverages, not duplicates DoD efforts and expertise. This bill, unfortunately, backtracks on the principles of the MOA, by expanding the size, scope, and reach of DHS and neglects to afford the authorities necessary to protect the homeland to the only institutions currently capable of doing so, U.S. Cybercommand and the National Security Agency (NSA).

At a recent FBI-sponsored symposium at Fordham University, General Keith Alexander, the Commander of U.S. Cybercommand and the Director of the NSA stated that if a significant cyber attack against this country were to take place there may not be much that he and his teams at either Cybercommand or NSA can legally do to stop it in advance. According to General Alexander, "in order to stop a cyber attack you have to see it in real time, and you have to have those authorities. Those are the conditions we've put on the table…Now how and what the Congress chooses, that'll be a policy decision." This legislation does nothing to address this significant concern and I question why we have yet to have a serious discussion about who is best suited to protect our Country from this threat we all agree is very real and growing.

Additionally, if the legislation before us today were enacted into law, unelected bureaucrats at the DHS could promulgate prescriptive regulations on American businesses – which own roughly 90 percent of critical cyber infrastructure. The regulations that would be created under this new authority would stymie job-creation, blur the definition of private property rights and divert resources from actual cybersecurity to compliance with government mandates. A super-regulator, like DHS under this bill, would impact free market forces which currently allow our brightest minds to develop the most effective network security solutions.

I am also concerned about the cost of this bill to the American taxpayer. The bill before us fails to include any authorizations or attempt to pay for the real costs associated with the creation of the new regulatory leviathan at DHS. This attempt to hide the cost is eclipsed by the reality that the assessment of critical infrastructure, the promulgation of regulations and their enforcement will take a small army.

Finally, I'd like to find out over the next few days what specific factors went into providing regulatory carve-outs for the IT hardware and software manufacturers? My suspicion is that this had more to do with garnering political support and legislative bullying than sound policy considerations. However, I think the fact that such carve outs are included only lends credence to the notion that we shouldn't be taking the regulatory approach in the first place.

Because of provisions like these and the threat of a hurried process, myself, and Senators Hutchison, Chambliss, Murkowski, Grassley and others are left with no choice but to introduce an alternative cybersecurity bill in the coming days. The fundamental difference in our alternative approach is that we aim to enter into a cooperative relationship with the entire private sector through information sharing, rather than an adversarial one with prescriptive regulations. Our bill, which will be introduced when we return from the President's Day recess, will provide a common-sense path forward to improve our nation's cybersecurity defenses. We believe that by improving information sharing among the private sector and government; updating our criminal code to reflect the threat cyber criminals pose; reforming the Federal Information Security Management Act; and focusing federal investments in cybersecurity; our nation will be better able to defend itself against cyber attacks. After all, we are all partners in this fight, and as we search for solutions, our first goal should be to move forward together.