Testimony
U.S. Senate Committee on Homeland Security and Governmental Affairs
Thursday, February 16, 2012,
"Securing America's Future: The Cybersecurity Act of 2012."
James A. Lewis, Center for Strategic and International Studies

Mr. Chairman and members of the Committee, thank you for the opportunity to testify. Congress has an important and defining challenge before it as it considers cybersecurity. This technology has profound implications for our economy and for our security, but law and public policy have not kept up. The laws and policies that were appropriate when the internet was a toy will not secure our nation as we become increasingly dependent on what has become a critical global infrastructure. We derive tremendous economic benefit from cyberspace, but it is also a source of unparalleled vulnerabilities for our nation, vulnerabilities that others have been quick to exploit.

Reducing risk and vulnerability in cyberspace is a fundamental challenge. In considering this problem, we have learned through painful experience that market forces will not secure cyberspace and that existing authorities are inadequate for national security and public safety. The list of private sector companies, including technology leaders, whose defense have failed is long and would be longer if all breaches were disclosed. Continuing to use voluntary, market driven approach to this new national security concern is irresponsible and guarantees a successful attack against our nation. The Committee has done our nation a service by taking on the challenge of cybersecurity. Unfortunately, Mr. Chairman and members of the Committee, while there are many good things in this bill in a few crucial areas it needs to be strengthened. As currently drafted, this bill includes significant loopholes that would keep our nation at risk.

Some of these loopholes are intended to accommodate industry concerns. These industry concerns are understandable and the bill makes reasonable efforts to accommodate them. However, in a few instances the language to assuage industry concerns goes too far and ends up putting national security at risk. As with any important regulation, there is a delicate balance between protecting the nation and minimizing burdens on our economy. This bill makes valuable strides in this direction and with a few changes, the Committee, the Senate and the Congress can find the balance that best serves the national interest.

In the long discussion leading up to this hearing, a number of objections have regularly been used to explain why it should be diluted or rejected. This is part of politics in a democracy and we will ultimately see truth emerge from debate. Ultimately, my hope is that we can find a pragmatic approach that protects the nation, but to do this we must hold some of the assertions about the risks of better cybersecurity up to the light and examine them more closely.

The strangest of these assertions is that we face no real threat in cyberspace, or that the threat does not warrant taking action, or that the defense industrial complex has inflated cyber threats to justify spending. Like any new trend in policy, cybersecurity has in the last few years attracted a wave of new scholars who are, in a sense, learning their trade by doing it. The field is fragile, hampered by poor data, weak research methodologies, inexperience and powerful ideologies. Cybersecurity also has a unique problem in that some of the most reliable data is classified. This

noisy debate is a symptom of the growing pains that societies experience as they adjust to a new technology. We are at an inflection point, however, when it comes to cybersecurity. The existing approach has failed and change is inevitable, either through our own efforts or after it is forced upon us by events.

I know you have been briefed by senior administration officials on the threat we face, and that those of you who have served on the intelligence oversight committees have a deep appreciation of the problem. But there are still many who either lack this knowledge or profess to be unconvinced. Even using only open source material, we can assess the growing threat to national security and public safety in cyberspace.

Many countries are building cyber-attack capabilities – a study last summer found thirty five nations developing military doctrine for cyber war. Two of the nations that are most advanced in cyber-attack capabilities are among our most likely military opponents – Russia and China. These nations bear us ill-will and their militaries and intelligence services have planned cyber-attacks against us. Barring some miscalculation, they will avoid cyber war but if there was a conflict with either nation, the U.S. is shamefully defenseless.

China and Russia are great powers with many interests and are unlikely to engage in frivolous attacks. They have instead taken advantage of our weak cyber defenses to engage in widespread economic espionage and crime. Other potential attackers may not be so restrained. When these less constrained attackers acquire advanced cyber-attack capabilities, the risk to the U.S. will increase significantly. The two most dangerous of these "acquiring powers" are Iran and North Korea, but anti-government groups, cyber criminals and perhaps jihadis may also be acquiring cyber-attack capabilities.

Iran has been seeking cyber-attack capabilities for years. We do not have a good understanding of Iranian capabilities, but Iran was probably responsible for hacking a Dutch internet company "Digi-Notar," to intercept communications from Iranian dissidents. This was a significant breach that put online commerce at risk. Iran has close military relations with China and Russia, who could assist it in developing cyber capabilities. Director of National Intelligence James Clapper testified recently that Iran is losing its reluctance to strike domestic targets in the U.S. Given its demonstrated willingness to use proxies for terrorist acts, Iran could decide that it is safe to launch a covert cyber-attack against our vulnerable infrastructure.

North Korea has been pursuing cyber warfare capabilities since the mid-1990s and Kim Jong-il, the former leader, had a deep interest in information warfare and ensured long term support for the DPRK military to acquire cyber-attack capabilities. North Korea routinely probes South Korean networks and may be responsible for several basic-level attacks. As with Iran, open source information on North Korean capabilities is limited, but we know they want cyber weapons and it is unwise to depend on the restraint of a nation that feels no compunction about shelling islands or torpedoing patrol boats.

Another potential source of cyber-attack comes from antigovernment or anarchist groups. This could include teenagers with a grudge, anarchists who wear black masks and smash shop windows in violent protests, cyber criminals, and perhaps even foreign intelligence services

attempting to use political groups as "cover." To date, most of the actions attributed to these groups have been a source of annoyance more than damage. But some in the hacker community say that some of the most skilled hackers in the world are among the ranks of Anonymous, a leading hacker group. We have some idea of their motivations, which are anti-government and anti-American, and of their inventiveness and skill, as they, like our nation-state opponents, have been able to exploit corporate networks with ease.

While the likelihood of cyber-attack is increasing, it is still unlikely that these attacks would cause mass casualties or catastrophic damage at a national or regional level. Attacks will likely resemble the Stuxnet attack, the 2003 Northeast Blackout, or the 2010 stock market "flash crash." Neither the blackout or the flash crash were caused by cyber-attack, but they were the result of computer failures and a shrewd opponent could duplicate these failures and exploit our lack of defenses to make incidents like these last weeks instead of a few days. I would note that in the Northeast Blackout, the "Flash Crash," of 2010, or even Stuxnet, there were no casualties, no mass evacuations. If we set the threshold for covered critical infrastructure as requiring mass casualties, mass evacuations, or national catastrophe, we may inadvertently be saying that we do not need to defend America against Stuxnet-like attacks.

It is important to focus new authorities on truly critical infrastructures, and to minimalize the effect of new regulation, but we should also bear in mind the nature of asymmetric warfare. When the threshold for identifying covered critical infrastructure uses terms like mass casualties, mass evacuations, or effects similar to weapons of mass destruction, we are essentially writing target lists for our attackers. They will attack what we choose not to defend. The critical infrastructure excluded from regulation will be the most likely target for attack.

Every critical infrastructure operator whose networks have been examined has been found to be vulnerable, and in many cases, examinations have found that opponents have spent months to "prepared the battlefield" for potential future strikes against America. Companies may not be aware of the threat and in any case, there are powerful and perfectly understandable economic disincentives for them to spend on public goods like national defense. We need to be cognizant of this and look for ways to allow companies to recoup costs. Not requiring them to improve their defenses, however, is a debacle waiting to happen, and better protection for critical infrastructure from cyber-attack is an immediate national concern.

We also know that America has been the victim of sustained and widespread campaigns of cyber espionage. The most technologically advanced companies in America have been no match for foreign opponents who have routinely and easily overcome private sector defenses. Companies, naturally, conceal their losses and may not even be aware of what has been taken. Government agencies, through their own activities, have an idea of what American firms have lost and have knowledge of the plans, intentions and capabilities of our most active opponents, but a welter of well-intentioned laws written in the 1980s to protect privacy hampers the ability to share this information among companies or between private sector and government. This bill, along with proposed legislation in the House, appropriately addresses the information sharing problem. This cyber espionage costs American jobs, damages trade competitiveness, and puts our technological advantage at risk.

Government agencies have also been the victim of cyber-espionage, but they have in the last few years undertaken a vigorous response that has improved their defense. The most notable examples of this is the creation of Cyber Command in response to the 2008 penetration of a classified military network and actions taken at the Department of State that have dramatically reduced opponent success rates. The section of this bill that address FISMA are important to solidify and continue this progress, but frankly, we have not seen similar progress in the private sector, where cyber defenses are uneven and exploitable.

Yesterday's Wall Street Journal's story on Nortel illustrates the problem. Hackers stole passwords form Nortel executives, including the chief executive officer. This gave them access to "technical papers, research-and-development reports, business plans, employee emails and other documents." The penetration lasted many years and Nortel "did nothing from a security standpoint" to end the penetration. We do not know how many other situations like Nortel are out there, but we do know that many Fortune 500 companies have been the victim of similar exploits.

As a nation, we are still too reliant on cybersecurity policies from the 1990s that depend on voluntary action, market forces and feckless public private partnerships. This approach has failed. It is inadequate for what has become a global infrastructure that our economy relies upon and, because of its speed and scale, makes criminals, spies and hostile militaries our next door neighbors. Continued endorsement of these old ideas as the basis for cybersecurity puts the nation at risk.

One common theme is that we need to keep cybersecurity weak to avoid damaging innovation. Innovation has become a kind of mantra in Washington, but our assessments of how to accelerate innovation are inadequate. We need a better understanding of the role of the Federal investment in education and research and its relation to the commercialization of new technologies by the private sector if we are to rebuild our innovation capacity. We need to improve the general economic environment and remove obstacles to the creation of new businesses – but there is nothing in this bill that creates such obstacles to innovation. Increasing America's ability to innovate is a serious concern, but to argue that this requires weak cybersecurity is nonsensical. Because of the ease of cyber espionage, our national spending on innovation is, in effect, a partial subsidy to foreign competitors: they share the fruits of our investments without having to pay for them.

The relationship between innovation and regulation is complex and is easily mischaracterized. Too much regulation or regulation that is too prescriptive will damage the ability of entrepreneurs to create new companies. Well-intentioned regulations, combined with badly designed fiscal and investment policies, slow American economic growth. Too little regulation, however, puts the public interest at risk. Events on Wall Street demonstrated this – America deregulated the financial sector, and then it crashed the global economy. Our current weak regulatory structure for cyber security puts us on track to repeat this mistake at the expense of national security. What is needed is a pragmatic, minimalist, and balanced approach to regulation. Finding this approach can be difficult, but the approach taken in Section 105 is, dare I say it, innovative, avoids prescriptive regulation and follows established commercial practices to create a minimalist regulatory structure that will, if the threshold for covered infrastructure

and the exclusions for commercial IT products are revised, will increase national security and serve the national interest.

In fact, well-designed regulation can spur innovation. The Federal Aviation Administration has far more intrusive and onerous regulation than what is envisioned in this bill. The FAA was established in 1958, but we have been able to move beyond propeller aircraft. Similarly, when car manufacturers testified decades ago before Congress on auto safety regulation, they said that Federal intervention to make cars safer would destroy the American auto industry. The American auto industry has had several near death experiences since then, but these have been self-generated rather than the result of burdensome regulation. Auto safety regulation created a competition among car manufacturers to innovate in building new safety feature. Regulation accelerated innovation in this case while saving thousands of American lives.

Some might say that aviation safety is more important than cybersecurity, but as the internet and digital applications move to the center of economic activity, this would be a grievous mistake. National security and public safety are burdensome, and can require burdensome regulation. But we should not pretend that avoiding the burden will somehow make us safe. There is a natural tendency in this discussion to exaggerate the costs of cybersecurity. Most studies of cost are regrettably inaccurate. Better cybersecurity may not entail any new cost, just change in how people spend. This would not be true, of course, if a company is currently spending little or nothing to secure its networks, but isn't this the problem we are trying to fix?

One question that comes up repeatedly is that we regulate flight and autos because a failure to do so would result in death, but we will not have cybersecurity regulations until someone dies. Many in the security and intelligence world believe we will not take cybersecurity seriously until there has been a disaster. This Congress has an opportunity to prove them wrong.

Some privacy advocates oppose stronger cybersecurity measures. The heart of this opposition is a distrust of government and a fear that new authorities will be misused. These are, frankly, reasonable concerns that can only be addressed by adequate oversight and clear rules and limits on how new authorities can be used. This oversight responsibility fails first on the Executive Branch and bodies such as the President's Civil Liberties Oversight Board, which is moving steadily towards realization, but ultimately it is the responsibility of the Congress. The measures in this bill, frankly, do not pose any real risk to privacy or civil liberties, but the legacy of Warrantless Surveillance continues to raise concerns that can only be addressed by a strong commitment to oversight and transparency.

There is a question of how far "upstream" in the industry DHS should have authority. Section 104 of the bill excludes all commercial software and hardware. I am not sure what this would leave, as I know of no freeware or open source industrial control systems or microprocessors. We do not want agencies telling Information Technology companies how they should write code, but carving out all "commercial IT products" risks seriously undercutting the positive effect of the bill.

Section104 needs to be clarified to ensure that owners and operators of covered infrastructure can be required to mitigate identified vulnerabilities. In particular, it needs to clarify that

existing guidelines on vulnerabilities can be applied to critical infrastructure networks. The intent of Section 104 is understandable. It seeks to shield the commercial information technology vendors from regulation and liability. Section 104 (b) (2) (c) makes sense. DHS should not be telling companies how to write code or design semiconductors.

But as drafted, the section seriously weakens the bill. It basically says that the Federal government cannot regulate or require any changes in commercial information technology, how it is installed, or how it is maintained. If commercial information technology products currently in use were secure, were installed securely and were maintained in that condition, this language would not be a problem. However, this is not the case. The blanket restrictions found in Section 104 (b) (2) (a) and (b) that forbid Federal agencies from regulating "related services, including installation services, maintenance services, repair services, training services, and any other services provided in support of the product" should really be called the "Huawei exemption." Installation, maintenance, and repair are prime attack vectors. Excluding these services from regulation is an open invitation to our most dangerous opponents.

An example of this problem was found in 2010 by security researchers examining smart grid technology. Smart grids will transmit information about consumer energy use and allow for better management of energy flows. Smart grid meters will encrypt information to protect it. One element of the encryption system would use a "random number generator," to scramble data. These are a standard element in many encryption programs. But random number generators are hard to create and can be expensive. So instead, the designers of some smart grid meters chose to use a fixed list of numbers from which the meter would randomly draw, a kind of poor man's random number generator. Unfortunately, astute teenagers could defeat this kind of encryption feature as early as the 1990s. But under Section 104, no federal agency or officer could ask for it to be changed or fixed.

You can get a sense of this by applying our FAA comparison. If this language applied to the FAA, it could not require an airline not to buy defective parts. It could not set the standards by which an airline would need to maintain its aircraft. If it learned of a problem, it could not require airlines and their suppliers to fix it. This is no way to run an airline and it is no way to defend a nation.

The effect of this language goes beyond critical infrastructure. It may undercut an important achievement from the Bush Administration in cybersecurity. Work at the U.S. Air Force found that secure operating systems settings would protect its networks against most cyber-attacks, as well as reduce cost. The Office of Management and Budget learned of this and issued a memorandum for other agencies to adopt this "Federal Desktop Core Configuration" - FDCC. Although the FDCC reduced cost and improved security, it was opposed by several IT companies and associations on the grounds that they were not adequately consulted and that the changes to a secure configuration would be costly. The objections slowed moving to more secure networks and the language in this section could have the effect of undoing or blocking the improvements now being used by Department of Defense and other agencies.

What exactly is the fear? If it is to avoid having DHS tell companies how to build their products, this is a reasonable concern that subsection c of the bill adequately addresses. If it is to avoid

liability for selling insufficiently secured products, this too is a long-standing industry concern that should be assuaged. But we need to find ways to restrict Federal interference in design and production and avoid creating new sources of liability without destroying the bill.

We do not want to limit the ability of the Federal government to establish standards for services in support of commercial technology used in critical infrastructure, including installation services, maintenance services, repair services, training services, and any other services provided in support of the product. Misconfiguration at the time of installation is a common problem and can create major vulnerabilities. Similarly, an opponent could use the remote update and maintenance services that are routinely provided to disrupt services or damage machinery. This is a real risk. This provision of the bill leaves the door open to disrupt critical infrastructure.

The Bush Administration's FDCC was just one of a number of developments in cybersecurity in the last few years that allow us to move a quantitative approach, where we can measure the effectiveness of security measures and significantly reduce risk. Anyone who tells you that we do not know how to do cybersecurity is sadly out of date. The National Security Agency, the National Institutes of Standards and Technology, and other Federal agencies are pioneering techniques that can strengthen America's defenses. But while we can require implementation and measure the rate of implementation in the Federal government, there is no comparable ability to measure and secure commercial critical infrastructure. This remains the single largest vulnerability for America in cyberspace. We still rely on haphazard policies and laws developed in the 1990s when the cyberspace was less important, critical infrastructures less vulnerable and the threats we faced smaller and the opponents less skilled.

This bill has much that is good in it. Other sections, on education, information sharing, research, international cooperation, and on how the Federal government secures its systems all make important contributions. Each deserves to be passed. But by themselves, or packaged together as a basket of low hanging fruit, they are inadequate to meet the risks we face today. The objective we all share of making America safer and more secure is in sight. Nonetheless, if this bill does not provide adequate authorities to mandate better cybersecurity in critical infrastructure, America will face increasing risk and an increasing probability of damaging cyber-attack.

I thank the Committee and will be happy to take any questions.