Statement of Ranking Member
Senator Susan M. Collins
"Securing America's Future: The Cybersecurity Act of 2012"
Thursday, February 16, 2012

★ ★ ★

After the 9/11 attacks, we learned of many early warnings that went unheeded, including an FBI agent who warned that one day people would die because of the "wall" that kept law enforcement and intelligence agencies apart. When a major cyber attack occurs, the ignored warnings will be even more glaring – because our nation's vulnerability has already been demonstrated by the daily attempts by nation-states, terrorists groups, cyber criminals, and hackers to penetrate our systems.

The warnings of our vulnerability to a major cyber attack come from all directions and countless experts, and are underscored by the intrusions that have already occurred. Earlier this month, FBI Director Robert Mueller warned that the cyber threat will soon equal or surpass the threat from terrorism. He argued that we should be addressing the cyber threat with the same intensity we have applied to the terrorist threat.

Director of National Intelligence James Clapper made the point even more strongly, describing the cyber threat as a "profound threat to this country, to its future, its economy and its very being."

Last November, the director of the Defense Advanced Research Projects Agency or DARPA warned that malicious cyber attacks threaten a growing number of the systems we interact with daily – like the power grid, water treatment plants, and key financial systems.

Similarly, General Keith Alexander, commander of U.S. Cyber Command and director of the National Security Agency, warned that the cyber vulnerabilities we face are extraordinary and characterized by "a disturbing trend, from exploitation to disruption to destruction."

These statements are just the latest in a chorus of warnings from current and former officials. The threat is not just to our national security, but also to our economic well-being. A Norton study last year calculated the cost of global cybercrime at 114 billion dollars annually. When combined with the value of time victims lost due to cybercrime, this figure grows to 388 billion dollars globally, which Norton described as "significantly more" than the global black market in marijuana, cocaine and heroin combined.

In an op-ed last month titled, "China's Cyber Thievery Is National Policy—And Must Be Challenged," former DNI Mike McConnell, former Homeland Security

Secretary Michael Chertoff and former Deputy Secretary of Defense William Lynn, noted the ability of cyber terrorists to "cripple" our critical infrastructure, and they sounded an even more urgent alarm about the threat of economic cyber espionage.

Citing an October 2011 report by the Office of the National Counterintelligence Executive, these experts warned of the catastrophic impact that cyber espionage – particularly espionage pursued by China – could have on our economy and competitiveness. They estimated that the cost "easily means billions of dollars and millions of jobs."

This threat is all the more menacing because it is being pursued by a global competitor seeking to steal the research and development of American firms to undermine our economic leadership. As the 2011 report by the U.S.-China Economic and Security Review Commission made clear, China continues to conduct a range of malicious cyber activities "to facilitate industrial espionage and the compromise of U.S. and foreign government computer systems."

The evidence of our cybersecurity vulnerability is overwhelming and compels us to act now. Some members have called for yet more hearings, studies, and mark-ups. In other words, more delay. The fact is, since 2005, our Committee alone has held 10 hearings on the cyber threat, including today's hearing. In 2010, Chairman Lieberman, Senator Carper, and I introduced our cyber security bill, which was reported by this Committee later the same year. Since last year, we have been working with Chairman Rockefeller to merge our bill with legislation he has championed, which was reported by the Commerce Committee. After incorporating changes based on the feedback from the private sector, our colleagues, and the Administration, we have produced a refined version, which is the subject of today's hearing. Chairman Rockefeller and Chairman Feinstein have also devoted countless months working on this vital issue. It is significant that three Senate chairmen with jurisdiction over cybersecurity have come to agreement on these issues. And each day we fail to act, the threat increases to our national and economic security.

Some of our colleagues have urged us to focus narrowly on the Federal Information Security Management Act, as well as on federal research and development and improved information sharing. We *do* need to address these issues – and our bill *does*.

However, with 85 percent of our nation's critical infrastructure owned by the private sector, the government also has a critical role in ensuring that the most vital parts of our infrastructure – those whose disruption could result in truly catastrophic consequences – meet reasonable, risk-based performance standards.

In an editorial this week, the *Washington Post* concurred, writing that our "critical systems have remained unprotected. To accept the status quo would be an unacceptable risk to U.S. national security."

Some of our colleagues are skeptical about the need for any new regulations. I have opposed efforts to expand regulations that would burden our economy. But regulations that are necessary for our national security and that promote – rather than hinder – our economic prosperity strengthen our country.

This bill reflects the extensive consultations we have had while still achieving the goal of improving the security of critical cyber systems. I look forward to discussing the bill with our witnesses today, and I thank the Chairman for calling this hearing and for the leadership he has shown on this vitally important issue.