Statement of Senator John D. Rockefeller IV

Senate Committee on Homeland Security and Governmental Affairs
Hearing on the Cybersecurity Act of 2012
February 16, 2012

Chairman Lieberman, Senator Collins, and distinguished Members of the Committee on Homeland Security and Governmental Affairs, I am honored to be here today to urge the Senate to move on the Cybersecurity Act of 2012.

It's an important bill, and I will fight for its passage. I look forward to the time when Secretary Napolitano and the Department of Homeland Security, which has made such important strides in this area, can begin implementing the protections that this bill provides for.

Our government needs a lead **civilian** agency to coordinate our civilian cybersecurity efforts, and that agency should be the one that has that responsibility now: The Department of Homeland Security.

I want to emphasize that our bill represents the expertise and hard work of three Senate Committees, and the input of many other Senators and outside stakeholders, over the course of the past three years.

We have eagerly sought – and have received – constructive criticism and input from all corners. Anyone and everyone who wanted to protect our country from the cyber threat had a seat at the table.

Even when people refused to engage with us, we tried to find their ideas and put them in the bill. A couple of weeks ago we took ideas from an op-ed that fellow Senators wrote.

Beyond this bill's principal authors – Senators Lieberman, Collins, Feinstein and I – this bill reflects the input, assistance, or requests of Senators on both sides of the aisle.

Senator Snowe was my co-author of the bill that Commerce reported out last year. Senator Carper was a co-author of the Lieberman-Collins bill. Both have left a major imprint on this bill, and I consider them partners in moving this ahead.

Senator Hutchison and her staff worked with us for a good part of the past two years, and we have tried hard to address all of her specific concerns. I think we have done so in virtually every case.

We have sought to engage Senator Chambliss, and before him, Senator Bond, in the same fashion.

Senators Kyl and Whitehouse contributed an entire title regarding cyber public awareness, and Senators Kerry, Lugar, Gillibrand and Hatch did the same on the title regarding diplomacy.

Because of Senator McCain's concerns, we omitted significant language pertaining to the White House cyber office.

And when colleagues had ongoing questions about a provision that I personally believe is extremely important, I agreed to drop it from the base bill. This provision would clarify private sector companies' **existing** requirements regarding what "material risks" pertaining to cyber have to be disclosed to investors in SEC filings.

I believe this provision is absolutely crucial for the market to help solve our cyber vulnerabilities and will fight for it as an amendment on the floor. But in the interest of providing more time to address colleagues' questions, I agreed to take it out of the bill that we introduced this week.

Any suggestion that this exhaustive process has been anything but open and transparent is **simply false**.

Why have we worked so tirelessly to include the views of all sides? Why have we tried so hard to get this right?

Because our country and our communities and our citizens are at grave risk. This is not a Republican or Democrat issue, it's a life or death issue.

I want to be clear: The cyber threat is a very real fact. This is not alarmism. Here's why:

Hackers supported by the governments of China and Russia, and also sophisticated criminal syndicates with potential connections to terrorist groups, are now able to crack the codes of our government agencies, our Fortune 500 companies and everything in between.

They are looting our country of our most valuable possessions on an unfathomable scale. But that's not the end of the problem.

The reason that this cyber **theft** is a life or death issue is the same as the reason that a burglar in your house is a life or death issue. If a criminal has broken into your home, how do you know all he wants to do is steal your belongings?

How do you know he's not going to hurt you or your family?

That's the situation we face right now. Cyber burglars have broken in, and they have destructive cyber weapons that could do us great harm.

That's why Admiral Mike Mullen, former Joint Chiefs Chairman, said that the cyber threat is the only other threat that's on the same level as Russia's stockpile of nuclear weapons.

And FBI Director Robert Mueller testified to Congress recently that the cyber threat will soon overcome terrorism as the **top** national security focus of the FBI.

Think about that – cyber threats will be as dangerous as terrorism. Cyber threats could be as devastating to this country as the terror strikes that tore apart this country just 10 years ago.

Think about how many people could die if a cyber terrorist attacked our air traffic control system and planes slammed into one another.

Or if rail switching networks were hacked - causing trains carrying people – or hazardous materials – to derail or collide in the midst of some of our most populated urban areas, like Chicago, New York, San Francisco or Washington.

We're on the brink of what could be a calamity on any given day – at a time that is not our choosing. That's why the Directors of National Intelligence under both President George W. Bush and President Barack Obama have said that the cyber threat is the number one threat to our country.

We can act now, and try and prepare ourselves. Or we can wait and face the consequences.

I'm here to argue that we should act now to prevent a cyber disaster.

That's what our bill would do.

It's premised on companies taking responsibility for securing their own networks, with government assistance where necessary. It focuses like a laser on protecting the most critical networks, and it promotes the innovation of the private sector market for information technology products and services.

This bill is a good product that has had its tires kicked for three years. It has already garnered significant praise from key industry groups and civil liberties advocates. I am very proud of what we have done.

We have a solemn responsibility to act before it's too late.

Ten years ago, throughout 2001, our national security systems warned us about the possibility of a terrorist threat. We know now that we failed to take sufficient action to address those threats. And we paid for it.

I think back to 2000 and 2001, when we saw signs of people moving in and out of our country, we saw dots appear to connect, and we knew something new and different and dangerous might be upon us.

Our intelligence and national security leadership took these matters seriously – but not seriously enough.

Then it was too late. 9/11 happened.

Today, with a new set of warnings flashing before us, and a wide range of new challenges to our security and our safety, we again face a choice.

Act now, and put in place safeguards to protect this country and our people. Or act later, when it is too late. I urge the Senate to act now.