FOR IMMEDIATE RELEASE

TOM CARPER

UNITED STATES SENATOR · DELAWARE

FOR IMMEDIATE RELEASE: Oct. 29, 2009
CONTACT: Katinka Podmaniczky (202) 224-2441

Statement of Senator Thomas R. Carper, Chairman

Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security

Committee on Homeland Security and Governmental Affairs

"More Security, Less Waste: What Makes Sense for our Federal Cyber Defense"

The issue of "Cyber Warfare" isn't science fiction anymore. It's reality. Over the past few years we have heard alarming reports that criminals, hackers and even foreign nations have deeply penetrated our government's most sensitive networks, including the offices of some of us right here in Congress. In fact, just last week the congressionally established U.S.-China Economic and Security Review Commission reported that China is strategically developing offensive capabilities that could be used against us in a future military conflict.

Further, there have been reports that some of the previously successful cyber attacks against agency networks may have left behind what's known as a "backdoor," essentially a technological means for the bad guys to get back into our networks without anyone knowing.

These vulnerabilities could be used against us by those who might want to do us harm by stealing sensitive information stored on military networks or shutting down critical networks when we need them the most. Imagine the terrifying scenario of a hacker creating uncertainty as to the validity of the data residing on the Federal Aviation Administration's Air Traffic Control systems.

That is exactly the kind of scenario I hope our hearing today helps prevent.

But, the threat of a cyber attack isn't something new. In fact, in 2002 Congress passed what is known as the "Federal Information Security Management Act" – or FISMA for short – to help prevent many of the problems we will be discussing today. FISMA brought greater attention to the issue of cyber security and helped establish greater accountability within agencies. Overall, it was a step in the right direction.

However, seven years after the passage of FISMA and approximately $40 billion later, I am troubled to learn that the Office of Management and Budget does not track how much agencies spend on cyber security or measure whether those expenditures actually resulted in improved security.

And even more troubling, agencies may be constrained from implementing the most basic of cyber security best practices because of inflexible requirements. Allow me to put that into perspective, federal agencies have spent more on cyber security than the entire Gross Domestic Product of North Korea, who some have speculated is to be involved with some of these cyber attacks.

That is simply unacceptable.

Some of the problems with FISMA implementation are a direct result of OMB's decisions over the years, while others are due to agency neglect. Still other problems lay at the feet of those of us here on Capitol Hill. In essence, we all share in the blame. However, at today's hearing we have an opportunity to discuss some concrete ways to correct some of those wrongs.

For example, one wasteful and ineffective area that OMB and agencies can target is what is known as the "Certification and Accreditation" process. A Certification and Accreditation is essentially a process whereby agencies evaluate every three years what defensive security protections are in place to prevent attacks on their key systems. The process costs taxpayers about $1.3 billion every year and it produces a good deal of paperwork that ends up stored in binders in some clutter-filled room.

If we look at the chart to my right, we can see three years worth of reports from the Department of State, which cost a total of $38 million dollars. These reports would be worth the price tag if the tactics that hackers used were as static as words typed on a piece of paper.

But hackers change how they attack us daily and their numbers continue to grow.

And yet it seems like OMB thinks that a snapshot of agency preparedness every three years will defend our critical networks. But instead, billions of dollars are spent every year on ineffective and useless reports, similar to the ones pictured here. Meanwhile, we continue to get attacked. However, testifying today will be a representative from the Department of State who saw an opportunity to spend his agency's cyber security budget more wisely.

Instead of spending money on ineffective paper-based reports, the State Department decided to focus on developing a system that monitored their global networks on a continual basis. If we take a look at the second chart on my right, we can see the results of their hard work. According to the State Department, they were able to reduce the amount of risk to their agency by 90 percent in a single year. I'm told that this was achieved by developing a system that makes sense, uses effective metrics, and holds people accountable. In essence, the Department of State can prove they have better security at a fraction of the cost.

So as we progress through the hearing, I would like our witnesses to keep in mind that moving to a model like the one at State Department requires no new legislation, cost less than or the same as the current paperwork-laden method, and will better protect our country. That's the kind of cyber security that makes sense.

In fact, my colleagues and I introduced a bill last session, and again this year, which would require all agencies to move to a proactive approach like the one the State Department has taken. In addition to requiring continuous monitoring of security controls and putting a strengthened Chief Information Security Officer in each agency, my bill would enhance the role of the Department of Homeland Security in cyber security. The department would share information with agencies on where cyber attacks have been successful so that they can better prioritize their security enhancements. Further, my bill would require agencies to use their enormous purchasing power to persuade vendors to develop and sell more secure IT products and services in the first place.

###