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

"Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?"

March 12, 2008

The Subcommittee will come to order.

My thanks to our guests and witnesses for being here today. This hearing marks what I hope will be just the beginning in our proactive efforts to secure one of our most threatened and important national resources: our sensitive information.

Every day our government's computers experience thousands of attacks by individuals seeking to gain access to our taxpayer records, medical records, Social Security numbers, proprietary business information, and military secrets. The public expects that agencies holding this information will take every precaution necessary to ensure that it is secure and well-protected. However, despite progress reported in the Office of Management and Budget's most recent report, I feel like we are still extremely at risk. Our inability to secure federal information networks and protect the information they contain leaves American citizens open to threats like identity theft. It even places our national security at risk

For example, according to a report released last Monday by the Department of Defense, the United States government and our allies around the world have come under attack in the past year by hackers from addresses that appear to originate from the Chinese government. These hackers were able to compromise information systems at government agencies, defense-related think tanks, contractors, and financial institutions. Germany's domestic intelligence agency, the German Office for the Protection of the Constitution, has accused China of sponsoring these attacks "almost daily" in an attempt to "intensively gather political, military, corporate-strategic and scientific information in order to bridge their technological gaps as quickly as possible."

The threat of a nation-state cyber attack is very real. Last year in Estonia, an attack by Russian nationalist was coordinated through online chat rooms and websites. This "Cyber War," as newspapers called it, shut down websites of Estonian organizations, including the Estonian parliament, banks, ministries, newspapers, and broadcasters.

But we don't have to look over seas to find threats to our information security. Sometimes, we only have to look in our own backyards. Just last year, the Veterans Affairs Department had an external hard drive stolen, exposing sensitive personal

information on close to 2 million individuals. But the Veterans Affairs isn't the only example. The Departments of Defense, Transportation, Commerce, Health and Human Services, Homeland Security, Education, Agriculture, and State were all compromised by current or former employees. These incidents are simply unacceptable. I have a feeling that if a private sector company, like a bank or insurance company, that is entrusted with sensitive data were as vulnerable as some of our federal agencies seem to be, they would be out of business pretty quickly.

The Federal Information Security Management Act, or FISMA, came out of a recognition a few years ago of the critical importance of protecting our information systems. Since then, agencies have made extraordinary progress in implementing crucial information security measures and they should be acknowledged and complimented for their efforts. However, I am concerned that, five years after the passage of FISMA, agencies may be falling into the trap of complacency and just checking boxes to show compliance with requirements written into a bill.

Once again, I would like to thank our guests for testifying today and I look forward to hearing how Congress can assist agencies in protecting our sensitive information from domestic and foreign threats.

Now, I would like to recognize Senator Coburn for his opening statement.