United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement for Chairman Joseph Lieberman
"Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century"
Homeland Security and Governmental Affairs Committee
June 15, 2010

The hearing will come to order. Good afternoon and thanks for being here today. Today, we're going to take a closer look at legislation Senators Collins, Carper and I introduced last week - the Protecting Cyberspace as a National Asset Act. It provides a comprehensive framework to modernize, strengthen, and coordinate our cyber defenses across civilian federal networks and the networks of the most vital privately-owned critical infrastructure – including some real basics of American life; our electric grid, financial systems, and our telecommunications networks.

Today, we're going to hear from the top cyber security official at the Department of Homeland Security, which of course has a critical role, responsibility, to play in protecting our cyber assets; and we're also going to hear from security and industry experts. We have, in preparing this legislation, consulted extensively with members of the Administration, people in the private sector, and privacy groups as well.

In the 40 years since the Internet was created, it has developed into a necessity of modern life, source of remarkable information and entertainment and commerce, and, as we also have come to know, it is a target of constant attack and exploitation. We know have a responsibility to bring the public and private sectors together to secure the internet, cyberspace, and secure it well. We believe that our bill would do just that.

The idea of "cybercrime" is not really totally new to the American people. We all know about identity theft and about emails from a foreign "prince," or "doctor," or "government official" who desperately needs to move some money out of his or her country and who will reward you richly – if only you'll give them your bank account number. Which some people actually do.

Identity theft and financial fraud are serious matters. But of course we need and we hope we through this bill to reorient our thinking about the risks inherent in the internet and cyberspace. Today we face much greater risks in cyberspace than crimes like identity theft. A sophisticated attacker could cripple most of our financial system, take down a lot of the electric grid, or cause physical devastation equal to or greater than conventional warfare. The fact is the threat of cyber attack is among the most serious threats America faces today.

President Obama has correctly described our sprawling government and private sector cyber networks as a "strategic national asset." But our efforts to secure those networks and that national asset have been disjointed, understaffed, and underfinanced. So, what does our bill do?

First, we need leadership, we need focused and clear leadership, and our bill provides it in the form of a White House Office of Cyberspace Policy that would lead all federal efforts to defend cyberspace. That is civilian defense and private. The office would be led by a Senate-confirmed director, accountable to the public. We have previously asked, for instance, White House cyber coordinator Howard Schmidt to testify before this committee but we've always been turned down, apparently, on the grounds of executive privilege. Our legislation would change that by requiring Senate confirmation and thereby making Mr. Schmidt or whoever holds that position subject to the call of Congress and the public.

We also need a stronger agency to defend the dot-gov networks and oversee the defenses of our most critical infrastructure. The Department of Homeland Security Inspector General will issue a report tomorrow critical of

many operational elements of the Department's cybersecurity effort, citing a lack of clear authority as one of the issues that needs to be rectified. Our bill more than addresses these shortcomings by creating a National Center for Cybersecurity and Communications within the Department of Homeland Security which would have new, strong authorities to protect non-defense, public sector and private sector networks from cyber attack. DHS already has this responsibility through presidential directive, but, in our opinion, insufficient authority to carry it out.

The sound defense of our cyber networks will only be successful if industry and government work together, so our bill will set up a collaborative process where the best ideas of the private sector and the government would be used to meet a baseline set of security requirements that DHS would enforce for the nation's most critical infrastructure.

Thanks to some excellent work by our colleague Senator Carper, our legislation reforms and updates the Federal Information Security Management Act to require continuous monitoring and protection of federal networks but do away with the paper-based reporting system that takes up time agencies really otherwise would be using and should be using to protect their networks.

Our legislation also would require the federal government to develop and implement a strategy to ensure that the almost $80 billion of information technology products and services that the federal government purchases each year--$80 billion--are secure and don't provide our adversaries with a backdoor into our networks. And of course if the federal government uses that $80 billion of purchasing power to drive security add-ons and innovations in information technology products it'll also be available and presumably bought by the private sector.

Finally, we would give special authority to the President to act in the event of a catastrophic cyber attack that could seriously jeopardize public safety or have disastrous effects on our economy or national security. In those instances, clearly defined in our legislation, the President could direct the National Cybersecurity and Communications Center at DHS to impose emergency measures on a select group of critical infrastructure to preserve those assets and the networks they rely on and protect the American people. These emergency measures would automatically expire within 30 days unless the President ordered an extension. I know there's been some concern and controversy about that provision and we can speak to it I hope in the question and answer period. But it's very important limitation on liability of private entities who take action in response to an order from the government and might otherwise incur liability. We protect them from that because the action the government is ordering them to take is in national security or economic interest.

So, freedom of expression and freedom to innovate are not inconsistent with greater security in cyberspace and that is exactly what we hope to combine and balance in this legislation.

Senator Collins.