Statement of

The Honorable Benjamin L. Cardin

United States Senator
Maryland
November 17, 2009

OPENING STATEMENT OF

SENATOR BENJAMIN L. CARDIN

CHAIRMAN, TERRORISM AND HOMELAND SECURITY SUBCOMMITTEE

OF THE SENATE JUDICIARY COMMITTEE

HEARING: "CYBERSECURITY: PREVENTING TERRORIST ATTACKS
AND PROTECTING PRIVACY IN CYBERSPACE

Tuesday, November 17, 2009

The subcommittee will come to order.

Today the subcommittee examines one of the most important subjects - and frankly one of the most complicated subjects - that Congress and the Obama Administration must address in the coming months, and that is cybersecurity. Today hearing is entitled "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace."

The internet was initially designed as a research tool for the sharing of information, and today has grown into one of the most remarkable innovations of the technological and information revolution. The internet has greatly expanded the dissemination of information to individuals across the planet, and has allowed for a greater and more robust exchange of ideas in our new digital global marketplace.

With these improvements comes many new dangers, however. Today Senators will hear testimony that describes a range of new technological challenges that threaten to undermine cybersecurity and the ability of governments, citizens, and the private sector to safely and securely use the internet. Today we will have a bit of an education for Senators about some new technological terms in cybersecurity, including botnets, targeted and blended phishing, spyware, and malware. Our current system allows criminals, hackers, and terrorists to exploiting the weaknesses of the internet to gain access to confidential and classified information. Such attacks could also manipulate, corrupt, or alter data that is being used to run critical information systems inside the government or private businesses.

Soon after taking office, President Obama ordered a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity. The review team of government

cybersecurity experts engaged and received input from a broad cross-section of industry, academia, the civil liberties and privacy communities, State governments, international partners, and the Legislative and Executive Branches. In May 2009, the CyberSpace Policy Review ("Review") summarized the review team's conclusions and outlined near-term and mid-term action items, for moving toward a reliable, resilient, and trustworthy digital infrastructure for the future.

This Review contained some sobering conclusions.

The Review stated that "the federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way."
The executive summary concludes that "the nation is at a crossroads...the status quo is no longer acceptable...the national dialogue on cybersecurity must begin today..."

It also stated that "the United States cannot succeed in securing cyberspace if it works in isolation...the Federal government cannot entirely delegate or abrogate its role in secure the Nation from a cyber incident or accident...working with the private sector, performance and security objectives must be defined for the next-generation infrastructure..."

Finally, the report states that "the White House must lead the way forward."

Today's hearing will therefore examine both governmental and private sector efforts to prevent a terrorist cyberattack, which if successful could cripple large sectors of our government, economy, and essential services. I note that the first recommendation from the Review was to "appoint a cybersecurity policy official responsible for coordination the Nation's cybersecurity policies and activities."

The hearing will also examine the proper balance between improving cybersecurity and protecting the privacy rights and civil liberties of Americans.

I note that another recommendation from the Review was to "designate a privacy and civil liberties official to the NSC cybersecurity directorate."

Finally, we will examine the proper role of government in setting standards for the private sector or taking control of the internet or computer systems in an emergency.

I look forward to the testimony of our distinguished panel of government witnesses on Panel 1, including the Department of Justice, Department of Homeland Security, National Security Agency, and the Federal Bureau of Investigation.

I also look forward to the testimony of our distinguished panel of outside witnesses on Panel 2, including the Center for Democracy and Technology, the Internet Security Alliance, and the U.S.-China Economic and Security Review Commission.

I will now recognize Senator Kyl, the Ranking Member of our Subcommittee, for any remarks that he would care to make at this time.