Opening Statement of
Senator Susan M. Collins

"Protecting Cyberspace as a National Asset Act of 2010"

Committee on Homeland Security and Governmental Affairs

June 15, 2010

★ ★ ★

The information revolution touches every aspect of our lives, from personal relationships and entertainment to commerce and national security information. Cyberspace is a place of great, even unparalleled, power, but also of great vulnerability.

Cyberspace is under increasing assault on all fronts. The cyber threat is real, and the consequences of a major successful national cyber attack could be devastating. As former Director of National Intelligence Michael McConnell testified in February, "If we went to war today, in a cyber war, we would lose."

Since the terrorist attacks of September 11, 2001, we have done much to protect potential targets such as ports, chemical facilities, and other vital assets. We cannot wait for a "cyber 9/11" before our government realizes the importance of protecting our cyber resources.

We are already under fire. Just this past March, the Senate's Sergeant at Arms reported that the computer systems of Congress and the Executive Branch agencies are now under cyber attack an average of 1.8 BILLION times per month. Cyber crime already costs our national economy an estimated $8 billion per year.

We must move forward now with an aggressive and comprehensive approach to protect cyberspace as a national asset. The vital legislation that we introduced last week would do just that, fortifying the government's efforts to safeguard America's cyber networks. It would build a true public/private partnership to promote national cyber security priorities.

For too long, our approach to cyber security has been disjointed and uncoordinated. This cannot continue. The United States requires a comprehensive cyber security strategy and strong coordination among law enforcement, intelligence agencies, the military, and the private owners and operators of critical infrastructure.

Our bill would establish an essential point of interagency policy coordination within the White House. The Office of Cyberspace Policy would be run by a Senate-confirmed Director who would advise the President. This Director would develop a national cyber security strategy.

To be clear, the White House official would not be another unaccountable czar. The Cyber Director would have defined responsibilities and be accountable to Congress. The Cyber Director would be an advisor and coordinator - not an implementer.

That responsibility, for federal civilian systems and private sector critical infrastructure, would fall to a strong operational and tactical partner at the Department of Homeland Security – the newly created National Center for Cybersecurity and Communications.

For its day-to-day operations, the Center would use the resources of DHS, and the Center Director would report directly to the Secretary of Homeland Security.

On matters related to the security of federal networks, the Director would regularly advise the President – a relationship similar to the Director of the NCTC on counterterrorism matters or the Chairman of the Joint Chiefs of Staff on military issues.

These dual relationships would give the Center Director sufficient rank and stature to interact effectively with the heads of other departments and agencies. These relationships would be critical for the Center Director to set, monitor compliance with, and enforce security policies for federal civilian systems.

As we have seen repeatedly, from the financial crisis to the environmental catastrophe in the Gulf of Mexico, what happens in the private sector does not always affect just the private sector. The ramifications for government and for the taxpayers often are enormous.

This bill would establish a public/private partnership to improve cyber security across private sector networks. Working collaboratively with the private sector, the Center would produce and share useful warning, analysis, and threat information with the private sector, other federal agencies, international partners, and state and local governments.

Best practices developed by the Center would be based on collaboration and information sharing with the private sector. Information shared with the Center by the private sector would be protected.

In cases where owners and operators are responsible for assets whose disruption would cost thousands of lives in mere seconds or multiple

billions of dollars, the bill would establish certain risk-based performance requirements to close security gaps.

These requirements, for example, would apply to vital components of the electric grid, telecommunications networks, financial systems, or other critical infrastructure systems that could cause a national or regional catastrophe if disrupted.

These owners and operators would be able to choose which security measures to implement to meet applicable risk-based performance requirements. This model would allow for continued innovation that is fundamental to the success of the IT sector.

The bill also would provide limited liability protections to the owners and operators of covered critical infrastructure that comply with the new risk-based performance requirements.

If a cyber attack were imminent or occurring, the bill would authorize the President to undertake emergency measures to protect the nation's most critical infrastructure. The President would be required to notify Congress in advance of the declaration of a national cyber emergency, or as soon thereafter as possible. These emergency measures would be limited in duration and scope. The bill does not authorize any new surveillance authorities or permit the government to "take over" private networks.

The legislation also would take advantage of the federal government's massive purchasing power to help bring heightened cyber security standards to the marketplace.

Finally, the bill would improve the recruitment and retention of a qualified federal IT workforce.

If hackers can nearly bring Estonia to its knees through cyber attacks, infiltrate a major defense program, and hack the computers owned and operated by some of the world's most successful private sector computer experts, we must assume even more spectacular and potentially devastating attacks lie ahead.

I look forward to moving our bipartisan, comprehensive cyber security legislation forward this Congress.

###