# RANKING MEMBER WILLIAM KEATING (D-MA), OPENING STATEMENT

## Committee on Homeland Security
## Subcommittee on Oversight, Investigation and Management

## *"America is Under Cyber Attack: Why Urgent Action is Needed"*

In 2007, Chairman McCaul along with Congressman Jim Langevin were named co-chairs of the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency. Since that time, he has been a leader on these issues.

Last month, he and I co-hosted a House-wide cybersecurity briefing that included an in-depth discussion on how cyber attacks threaten our critical infrastructure, cell phones, and computers.

I am pleased to see that two of the participating organizations in that briefing - CSIS (The Center for Strategic and International Studies) and Northeastern University - are testifying today.

I look forward to continuing to work with Chairman McCaul on cybersecurity issues and performing oversight of the Department's role as the lead cybersecurity agency.

Cybersecurity, as acknowledged by President Obama, is "one of the most serious economic and national security threats our nation faces."

The impact of a cyber attack against critical infrastructure or our widely used federal system are spurring efforts in Washington to compel energy companies, along with other operators of vital infrastructure, to do more to protect their computer networks from hackers. Public reports reveal that Federal networks have been under attack for years. And, some accounts point to upwards of 3 billion cyber attacks a year in the US.

And, the price of security is not cheap.

Government agencies would need to boost cybersecurity spending more than seven times to block 95 percent of hacker attacks, according to a Bloomberg Government study. That translates into annual average spending of $190.3 million per agency, up from the current $26 million, according to the study based on interviews with officials of 48 federal, state and municipal agencies.

Moreover, one recent study estimated that 71 percent of all companies experienced a cyber attack last year.

The current combined financial impact on public and private sector cyber attacks is unknown but estimates are in the billions.

Yet, as we add up the dollars and weigh the risks, we must not forget that the greatest attack will be on the confidence of the American people if even one large-scale cyber attack scenario were to materialize.

It is therefore imperative that we get a full understanding of the root causes of cyber attacks, learn from where the threat is derived, and ensure that every available means of protection is deployed and at our disposal.

Mr. Chairman, last week during our full committee's mark-up of the PRECISE Act, I proposed an amendment that would have incorporated the model of the three legged stool of government working in partnership with academia and industry into legislation designed to anticipate cyber threats and develop means to combat them.

I plan to work further on this initiative because even in times of greatly needed cost-saving measures, we should be weary of trading in long-term gains for short term cuts. For this reason, our government should do more to accelerate the pace of research, discovery and development in homegrown technologies.

I believe that this path forward will enable us to see a return on our investments and remain competitive in the global economy, as well.

I know that my colleague, Chairman McCaul is a proponent of engaging research institutions on these matters and I congratulate him on his work on the Cybersecurity Enhancement Act of 2011.

Unfortunately, this week, the House will also consider legislation that contains broad and ambiguous language, serious privacy implications, and moves away from the Department of Homeland Security being the central agency for cybersecurity efforts.

The Department, through its United States Computer Emergency Readiness Team, or U.S. CERT, has made great strides and I am concerned that legislation compromising its authority will set us back in our fight against cyber attacks.

The President, the CSIS Commission on Cybersecurity for the 44th Presidency and the House Republican Cybersecurity Task Force have all made numerous recommendations on how to improve cybersecurity.

I would encourage my colleagues to bring legislation to the floor that fully protects constitutional rights and contains recommendations made by these entities.

I look forward to today's testimony and I am especially eager to hear from Dr. Stephen Flynn of Northeastern University as he discusses the nature of the cybersecurity threat and his standpoint on making universities full-fledged cyber security partners.