Opening Statement for Ranking Member Keating
March 21, 2013, 9 a.m.
EE & ET: Cyber Attacks: An Unprecedented Threat to U.S. National Security

- Thank you, Mr. Chairman for holding today's hearing.

- During the highly-publicized Benghazi hearing earlier this year, Secretary Clinton warned this Committee that cyber threats would be at the top of our agenda in the coming months. She was certainly correct.

- With the number of cyber threats escalating worldwide, the need for comprehensive security analysis, assessment, and actions has never been greater.

- Although cyber attacks and instances of cyber espionage are receiving a great degree of media attention and are undoubtedly increasing and evolving at a rapid rate, cyber threats are not a new phenomenon.

- The Government Accountability Office (GAO) designated federal information security as a high-risk area in 1997, and in 2003 expanded this area to include protecting our nation's critical infrastructure.

- Ten years later, just this February, it was President Obama that signed an executive order to facilitate information sharing about emerging threats and solicit new, voluntary cybersecurity standards for the nation's power grid, financial sector and other key institutions.

- Yet, 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.

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

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

- As a former District Attorney, I believe that our country's efforts toward deterrence and response to a known cyber attack do matter, even if we are not always sure who the aggressor is, their motive is or where they might be.

- While the issuance of the Executive Order is a welcome development, it will take responsible, legislative action to fully address cyber threats and vulnerabilities to critical infrastructure, and time is of the essence.

- Further, the internet is an open, international domain, and cyber crimes clearly go beyond the traditional law enforcement model.

- For this reason, national policies are incomplete without firm international cybersecurity standards and norms between like-minded allies.

- The US recently played an incredibly constructive role during the World Conference on International Telecommunications (WCIT) and beat back proposals by Russia, China, Saudi Arabia, and others

that sought to explicitly extend International Telecommunications Regulations (ITR) jurisdiction over the Internet.

- Unfortunately, the US also does not participate in many of the concrete initiatives put forth by the International Telecommunications Union (ITU) and other international organizations. However, these efforts further the connectivity and interoperability of the world's telecommunications networks, which, in turn, enhance American defense and intelligence communications capabilities.

- Also, just this week, NATO Secretary General Rasmussen was in Estonia. As most of us here know, Estonia experienced devastating cyber attacks directed from Russia at its Parliament, ministries, banking system, newspapers and broadcasters in 2007. This week's NATO meeting alluded to these attacks and highlighted the importance of moving on to an interoperability paradigm between like-minded allies.

- I would agree that more thought and discussion should go into NATO's cybersecurity efforts.

- Again, I am thankful for the participation of all our witnesses here today and look forward to hearing their thoughts on our current cyber state of affairs as well as ongoing cyber espionage efforts and attacks stemming from China, Russia, Iran and others.

- Before I close, I would note that this hearing is taking place at a time when the effects of arbitrary, across-the-board spending cuts are just beginning to be realized. I look forward to hearing from you, Mr Painter, about how the sequester and the perpetual uncertainty around budgeting impacts our Nation's cybersecurity efforts.