Opening Statement of the Honorable Marsha Blackburn
Committee on Energy and Commerce
Hearing on "Cyber Threats and Security Solutions"
May 21, 2013

(As Prepared for Delivery)

American companies, the U.S. government, and private citizens are facing new challenges in the fight to protect our nation's security, economy, intellectual property, and critical infrastructure from cyber attacks. Today the Energy and Commerce Committee is exploring how the private sector and our government are responding. We will also review the implementation of the President's Cybersecurity Executive Order 13636.

Cyber attacks have grown in scope and sophistication to include nearly every industry and asset that makes America work. That is why this committee is well-positioned to lead, oversee, and review policies and solutions to these wide-ranging and evolving threats. Last year an al-Qaeda video surfaced calling for a covert cyber jihad against the United States. On Sunday the New York Times reported that hackers sponsored by China's People's Liberation Army have resumed attacks on U.S. targets. According to the GAO, the number of cyber incidents reported by federal agencies to US Computer Emergency Readiness Team has increased by 782 percent over 6 years.

As vice chairman of the full committee, I offered a discussion framework – the SECURE IT Act – to provide our government, business community, and citizens with the tools and resources needed to protect themselves from those who wish us harm. The five major components that make up the Secure IT Act are: 1) allow the government and the private sector to share cyber threat information in a more transparent fashion; 2) reform how our government protects its own information systems; 3) create new deterrents for cyber criminals; 4) prioritize research and development for cybersecurity initiatives; and 5) streamline consumers' ability to be notified when they are at risk of identity theft and financial harm.

One of the things we know is that cybersecurity is uniquely ill-suited for federal regulation. Rapid changes in technology guarantee the failure of static, prescriptive approaches. Our focus should be on developing consensus public policy that puts American businesses in the driver's seat and allows cooperation and collaboration, not top-down and one-size-fits all mandates.

NIST's written testimony on implementing the framework of the Executive Order states, "Any efforts to better protect critical infrastructure need to be supported and implemented by the owners and operators of this infrastructure. It also reflects the reality that many in the private sector are already doing the right things to protect their systems and should not be diverted from those efforts through new requirements." Private solutions – not government presumptions – offer the best prospect for our future cyber defenses.

As we explore ways to incentivize the private sector to diminish our exposure to cyber threats, we must ensure the Executive Order stays true to a voluntary, cooperative standard. Likewise, Congress and the executive branch should refrain from further exploring legislative regulatory proposals giving DHS authority to impose critical infrastructure requirements as our government is purportedly already in the midst of working with the private sector to draft a voluntary cybersecurity framework.

I look forward to the testimony and appreciate all nine of our witnesses' thoughtful answers to our questions this morning.

###