Opening Statement of the Honorable Marsha Blackburn
Subcommittee on Communications and Technology
Hearing on "Promoting Security in Wireless Technology"
June 13, 2017

(As prepared for delivery)

Welcome to the Communications and Technology Subcommittee's hearing titled "*Promoting Security in Wireless Technology*". Thank you to the witnesses for appearing to offer your testimony on this important issue. Mobile connectivity has become essential to our daily lives as a result of advances in technology and consumer demand. Unfortunately, increasing reliance on wireless devices and networks has provided more avenues for cyber criminals to compromise our security and harm consumers.

According to the 2017 Hiscox Cyber Readiness Report, cybercrimes cost the global economy approximately $450 billion and over 100 million Americans had their medical records stolen in 2016. Threats to mobile devices and networks can run the gamut from the use of ransomware and phishing schemes to packet sniffing and attacks on encryption protocols used to protect information sent over wi-fi. These incidents have been occurring with alarming frequency on scales large and small. The Harvard Business Review wrote last September 22nd that "*mobile devices are one of the weakest links in corporate security*" and that "*if mobile security isn't a problem for your company yet, it will be*".

Hackers are smart and they are adapting. McAffee's 2016 Mobile Threat Report notes mobile devices are quickly becoming the cybercriminals target of choice because of the abundance of sensitive information individuals store on them. This is corroborated by a Newsweek report from March that stated mobile ransomware attacks have already grown over 250 percent in 2017. The sophistication and

frequency of cyberattacks against mobile devices continues to escalate and we must meet this challenge head on.

Our hearing will also examine threats to wireless networks. As the Majority Memorandum notes, mobile devices generate numerous air interfaces to transmit data, with each interface creating unique security vulnerabilities and attack methods. Threats include packet sniffing, rogue access points, jamming, and locating flawed encryption algorithms. These attacks can be initiated by hackers to obtain financial information, user passwords, and block legitimate network traffic. A recent example of this was the DDOS attack against Dyn which disrupted websites such as Twitter, Netflix, and Etsy last November.

I have often said that cyberspace is the battlefield of the 21st century. We must act now. Hard-working taxpayers are demanding leadership from Washington in the cyber arena and it is our duty to provide it. Enhanced defensive capabilities should be developed by promoting greater collaboration between public and private entities. CTIA has shown leadership through its Cybersecurity Working Group. Their efforts have brought federal agencies such as the FCC and DHS together with the private sector to develop solutions to the cybersecurity dilemma.

Whether it is encryption, the use of authentication standards, updating operating systems, or rigorous implementation of anti-virus software – we must have an "*all of the above*" approach when it comes to forging defensive strategies that will defeat and deter cyber criminals.

Thank you and I look forward to the testimony of our witnesses.