

**Opening Statement of Chairman Marsha Blackburn
Subcommittee on Communications and Technology hearing:
“Telecommunications, Global Competitiveness, and National
Security”**

May 16, 2018

Welcome to today’s subcommittee hearing entitled: “Telecommunications, Global Competitiveness, and National Security.”

Our country’s information technology sector is one of the best economic growth engines the world has ever seen. It allows people to communicate, be entrepreneurs, and pursue educational opportunities; it fosters greater efficiency across every sector of the economy. As I’ve said before:

Information is power, and history makes clear that countries with the best communications have a competitive advantage.

Moreover, our nation’s defense – the men and women in uniform who serve our country – depend on communications. U.S. military superiority is built upon intelligence, surveillance, and reconnaissance, and the communication of this information to outmaneuver potential adversaries.

The purpose of today's hearing is to understand the nexus between telecommunications and national security in a global context.

These are issues this Subcommittee, and the Energy & Commerce Committee more generally, understand well. In 2013, I authored a bill – H.R. 1468, SECURE IT – to promote greater voluntary sharing of cyber threats between the government and the private sector, as well as among private sector companies.

I was pleased that many of the provisions I authored were signed into law in 2015.

Additionally, the National Institute of Standards and Technology, or “NIST,” has also taken great strides to collaborate with the private sector on developing a voluntary Framework of cybersecurity best practices. Last month, NIST published the latest version of its Framework to be even more informative and useful to a broader array of stakeholders.

In today's world, where information literally travels at the speed of light, and new innovations are brought to market at a dizzying pace, it is critically important to leverage robust information sharing about threats and vulnerabilities.

This should include greater information sharing about the supply chain of hardware and software that make up our communications networks.

When it comes to the supply chain, we must think about it over the long-term. We are fully aware of the issues that the President has raised regarding China, Huawei, and ZTE. We are also aware that the Department of Commerce has serious concerns. This point merits discussion, and it is the reason our hearing is so timely.

The quick and easy route would simply ban foreign vendors of vulnerable hardware and software from accessing our markets.

But the marketplace for hardware and software is global, and a hallmark of the communication industry is scale.

In time, it will be difficult for our domestic communications providers to obtain their network infrastructure from trusted sources when vulnerable foreign vendors acquire more and more global market share.

What are the implications of all this to our nation's cybersecurity?

What are the implications for the race to 5G?

What are the broader implications to our economy?

And, most importantly, what are thoughtful solutions to such a complex problem?

These are some of the questions today's hearing seeks to address.

I am pleased to convene this hearing.

I look forward to the testimony of our witnesses.

And I yield 1 minute to the Subcommittee's Vice Chairman, Mr. Lance.