Security Vulnerabilities Within Our Communications Networks:
Find it, Fix it, Fund it
June 27, 2019
Opening Remarks of Commissioner Geoffrey Starks

Good morning everyone and thank you for joining me for this important discussion about securing our communications networks. If you are here, you have likely heard me talk about this issue and my view that we need to Find insecure equipment in our networks, Fix the problem, and help Fund the process. Find it. Fix it. Fund it

I'm particularly concerned about the threat posed by insecure equipment. These threats don't just affect individuals or businesses—they go to the fundamental notion of protecting our nation. Network Security is National Security, and our interconnected networks are only as secure as their most vulnerable pieces.

Current efforts by the FCC, with its supply chain proceeding, by Congress, with the NDAA prohibiting government procurement of telecommunications equipment from certain Chinese companies, including Huawei and ZTE, and by the Administration, with the May Executive Order barring U.S. companies from buying foreign-made telecommunications equipment considered to be a national security risk, have taken steps toward prohibiting or restricting insecure equipment going forward. And I applaud those steps. But those actions do not address a critical problem—this equipment is already in our networks. The threat is real, and it's already here.

And we need solutions. We cannot treat this issue asymmetrically –focusing strictly on how to keep insecure equipment with a national security risk out of our network going forward but failing to address the equipment already in our infrastructure.

This issue is of great importance to me, and it is important to bring as much expertise as possible in thinking through these complex issues. So, I am excited for today's gathering of

stakeholders—including carriers, manufacturers, academics, and industry experts--all in an effort to start crafting and developing a practical path forward.

I'm not the only one thinking hard about these issues. I'd like to recognize and welcome staff members from both the U.S. House and Senate who are with us this morning. I am glad that members of Congress are engaged on this issue and look forward to working together with them.

This forum is fitting because solving this issue is going to require public-private partnership. For example, we are going to need private carriers with insecure equipment in their network to come forward and raise their hand so that we can work with them to help fix the issue. For the carriers present here today, thank you for your leadership. Likewise, this issue is going to require a whole of government approach that deploys our technical and national security expertise, and quite likely a funding package that drives the result we all want – secure communications networks. During this workshop, I want us to really break down and dig in to what it will take to Find the insecure equipment, Fix the problem, and help Fund the process.

We will begin today with a description of the threats of having insecure equipment, including Huawei equipment, in our networks presented by Mr. Jim Lewis and Professor Jonathan Mayer.

These presentations will set the stage for our discussions for the remainder of the morning. Our first panel will explore the scope of the threats and risks posed by insecure equipment currently in our communications networks. We need to know where in the U.S. this equipment is located. We also need to consider what equipment poses a threat. There is an active debate over whether all Huawei equipment poses a threat, or whether some of it is safe or could be made safe and these are some of the issues I hope we will explore.

The second panel will focus on how to fix the problem. We need to transition carriers away from insecure equipment as rapidly as possible. While mitigation of risks may be possible, a "rip and replace" approach might be necessary. No matter what, we must minimize disruption to consumers. We must consider the options and what will be best for Americans who rely on these networks.

Finally, our third panel will discuss how to fund a solution. We can't expect carriers to replace insecure equipment alone. This is a national problem and it needs a national solution. Many of the carriers who purchased this equipment are small and operate in rural areas and may not be able to cover the costs of replacement without financial support.

Recent legislation proposes to allocate $700 million to fund the problem, and another estimate claims the cost could be over a billion dollars, depending on what equipment needs to be replaced, the timing of the replacement and other variables.

That's a lot of ground to cover today. One thing is clear – we can't afford to compromise our national security. So let's get started. The security of our networks depends on it. First up, Jim Lewis is a senior vice president at the Center for Strategic and International Studies. He has deep experience on these issues as a foreign service officer and as political and military advisor, among numerous other roles. He has testified before congress on many occasions and is an internationally recognized expert on cybersecurity. After him will be Jonathan Mayer, a professor of computer science and public policy at Princeton University. Professor Mayer was formerly the Chief Technologist in the FCC's Enforcement Bureau. His research focuses on understanding, at a technical level, the nature of threats presented by insecure equipment in communications networks. He is also researching technological means of identifying insecure equipment in networks.

Jim, I am honored to have you kick us off this morning.