NATIONAL SECURITY KEYNOTE REMARKS OF
COMMISSIONER GEOFFREY STARKS AT THE
5G RURAL ENGAGEMENT INITIATIVE
DENVER, CO
OCTOBER 30, 2019

Good afternoon, I'm FCC Commissioner Geoffrey Starks. Thank you very much for inviting me to spend time with you here today. Thanks especially to the U.S. Chamber of Commerce and to the Competitive Carriers Association for organizing this gathering today. I traveled nearly 6,000 miles overnight to be here today - coming straight to Denver from Sao Paulo. But here's the key – it's not because I'm that important, because I'm not. It is because you are that important. This national security conversation is that important, and I wanted to be a part of it. This gathering represents the core of the "all of government" approach to address 5G security concerns. With key leaders from the Department of Homeland Security, the National Security Division of the Department of Justice, and the National Telecommunications and Information Administration, this group, along with participating device manufacturers and service providers, represents an important gathering to consider the issues of 5G networks and ensure that they are secure. These conversations are essential to chart a path forward that will ensure secure networks. This is critically important – our networks touch every sector of our economy – so, to the extent they have vulnerabilities, those vulnerabilities are spread everywhere and affect nearly everything.

During my time as a Commissioner, I've tried to get outside the beltway as much as I can to meet people like you who are running the companies that are connecting Americans. Getting people connected is my highest priority and I thank you for your work making it happen. You all also happen to intersect with another priority of mine – network security. So, this afternoon I want to talk about how wireless networks have changed our lives and also about the threats that

come with them, how those threats have evolved, and the U.S. Government responses to address them. I also want to talk about my vision for what needs to be done to address network security concerns in the U.S. in addition to the work underway by other parts of the government. And, spoiler alert, the bottom line for me is that I think that we need to address, in a serious way, security problems that are present in our networks now.

I worked on National Security issues as Senior Counsel to the Deputy Attorney General at the Department of Justice, and have been drawn to these issues as a Commissioner. During my 10 months, I have raised a number of national security issues including concerns posed by undersea cables that make a direct connection between the U.S. and China, and threats that foreign actors are posing to our elections.

Last month, I was honored to have the opportunity to address the annual convention of the Competitive Carrier's Association in Providence, Rhode Island. (Thanks Alexi for inviting me!) While talking to CCA members at that event, I pointed out a developing issue involving the plan to construct an undersea cable between Los Angeles and Hong Kong. This project, which is backed by major U.S. companies and China's fourth-largest telecom provider, could end up carrying a large portion of the communications between the U.S. and Asia. The Justice Department is worried that communications over the cable could be stolen, blocked or modified on its Hong Kong end, and is consulting with other agencies about their recommendation to the FCC.

For my part, I'll decide my position once I have assessed the full record to determine whether any proposed outcome protects the national defense and the safety of life and property – which is the FCC's statutory direction in this area. Where there are national security issues raised with regard to our networks, I will do everything in my power to keep Americans secure.

On election security, just last week, I gave a keynote presentation to the 2019 Mobile World Congress in Los Angeles and raised the issue of election security as an immediate challenge where the stakes are high and so is the threat of outside influence. FBI and DHS documents suggest that Russian-affiliated cyber actors targeted election systems in all 50 U.S. states in the runup to the 2016 election. And there is every reason to believe that they have the means and motivation to do it again in 2020. Because of these risks, I have reached out to the major wireless carriers to discuss how they're hardening their networks to protect the integrity of our elections. This is another area where I will be using my position as an FCC commissioner and raising my voice. I'm committed to doing everything I can to secure our elections.

Above all of these, though, I have focused my time on the specific threat posed by insecure equipment, primarily equipment manufactured and supported by Chinese companies, in U.S. communications networks. I have been talking about this issue, and, specifically about the need to find insecure equipment in our networks, work with other policymakers to fix the security problems, and fund a solution for affected carriers – Find it, Fix it, Fund it. I first set this concept out in on an op-ed in The Hill in late May of this year, just weeks after the President issue his Executive Order barring U.S. companies from buying foreign-made telecommunications equipment deemed a national security risk. And, in June of this year, I held a workshop at the FCC to bring together carriers, equipment manufacturers, national security experts, academics, and other stakeholders to consider the issue of insecure equipment in U.S. telecommunications networks and my proposed "Find it, Fix it, Fund it" approach. This was the largest gathering of its kind ever held and it drove home several key points including that one of the most important questions to ask when evaluating whether a piece of communications equipment is trustworthy is whether the manufacturer is trustworthy. If they are not, the

consensus at the June workshop was that, due to the myriad paths to exploit networking equipment, it's unlikely that any equipment from a supplier that is not trusted could ever be trusted.

Between my June workshop and a second meeting with rural carriers with Chinese equipment in their networks at the CCA Conference in September, I am proud to say that I have met with nearly two dozen carriers with Chinese equipment in their network. Many communications networks in the U.S. and around the world have components manufactured and serviced by Huawei and ZTE. And, security experts around the world agree that use of this equipment presents significant security risks due to inconsistencies in the equipment's software code, and, more broadly, due to these manufacturers managing the networks, including creating and distributing software updates and patches, from China. An additional concern that amplifies remote management worries is that Chinese manufacturers are obligated, under Chinese law, to cooperate with Chinese government direction or requests to use networks assets for espionage or for other harmful purposes potentially including disrupting critical services or conducting cyber-attacks. The risk that network equipment could be used for surveillance and other malicious purposes tips these concerns from narrow considerations about attacks on a single service provider or network into much broader national security concerns. Unfortunately, concerns about these kinds of attacks are now the realities of the connected and dangerous world we live in. Network security is national security.

The nature of 5G networks also gives rise to new concerns. In earlier networks, "edge" elements could be separated from the "core" network, and lower security at the "edge" of networks was potentially tolerable as long as the "core" was protected. But 5G architecture, with significant network intelligence distributed throughout network components, makes such

distinctions impossible. Unlike earlier generations of wireless technology, the "core" and "edge," and all elements of 5G networks must be secure. Accordingly, though 5G networks are capable of supporting more sophisticated security measures, they also present a larger attack surface. To put a finer point on this, equipment manufactured and supported by Chinese companies has a wide open "front door" through which it receives updates from China in order to stay "secure" and to continue working. It may also have "back doors" either intentionally created or discovered due to software inconsistencies. But with the "front door" wide open, the secrecy of a stealthy "back door" becomes less important. With that in mind, I believe that U.S. service providers need to take these serious threats into account when considering whether to replace existing insecure equipment and, on what timeline to do so.

Some service providers I have heard from have been interested in exploring monitoring their Chinese-manufactured equipment as a means to mitigate threats. The theory is that constant monitoring will allow service providers to know immediately if "bad" or unexpected data is entering or leaving their network equipment. A "monitoring" approach raises several issues. First, "densified" 5G networks will have many, many antennas and radios. This means that monitoring would likely be an impossibly huge task. But second, and more importantly, a monitoring solution assumes that network equipment can be trusted, given proper monitoring, even if you don't trust the equipment manufacturer.

However, if an equipment manufacturer is not trusted, then every single aspect of the network that manufacturer produced, every piece of equipment it touches, and every software update and patch it designs could contain malicious code or present exploitable vulnerabilities. While the ability to trust the equipment is important, the ability to trust the supplier is critical.

And, I have come to think of monitoring in the absence of trust of the manufacturer as unlikely to give an acceptable level of confidence that network equipment is secure.

So, with these threats identified, one might fairly wonder – what's the U.S. government doing about it? The answer is - a lot. One example is this meeting here today. This gathering, and the significant government participation in it, is part of a serious and important "all-of-government" effort to ensure that our networks are secure.

Earlier this year, the President signed an Executive Order barring the purchase or use of equipment produced by an entity controlled by a "foreign adversary," recognizing them as creating an "undue risk of sabotage." This Executive Order assigned duties to various Federal agencies and work to implement it is underway across government agencies, including those in this room. Congress has also passed a defense appropriations bill in August 2018 that included a ban on government purchasing equipment from companies deemed insecure, including Huawei and ZTE. For its part, the FCC has proposed a ban on using the funds its universal access programs provide to purchase equipment from suppliers considered a security risk. Just this week the FCC announced that it will vote, later this month, on this proposal.

Each of these efforts is important, and all share a common goal of securing U.S. networks from bad actors, but they are also each focused on what to do in the future about security threats in communications networks. I have consistently said that we can't think of this issue asymmetrically, only focusing on keeping insecure equipment out going forward, and failing to address the insecure equipment located in U.S. communications networks today and that it represents a threat – today.

My view is that we must find this equipment, figure out what must be done to fix the threats that it poses-and every indication points to a solution involving replacing the equipment,

and we must look toward securing Federal funding to help carriers who have this equipment replace it. Find It, Fix It, Fund It.

When you talk with and really listen to the small rural carriers with Huawei or ZTE in their network, you hear two points. First, at the time when these telecom providers bought Chinese equipment, they did nothing wrong and broke no laws for which they should be punished. I agree. Second, you hear from these providers that—given their budgets—they are going to need assistance in paying for any replacement costs. On this account as well, I agree. Just last month, bipartisan legislation was introduced in the U.S. House of Representatives that would establish a $1 billion fund for small and rural wireless providers to use in replacing suspect equipment. Similar legislation was approved by the U.S. Senate's Commerce Committee earlier this year.

I know that ripping out Chinese equipment and replacing it with trusted equipment won't be turn-key, but I also know that we are talking about national security and that this isn't something we can afford to do on the cheap. And, I know there are multiple issues to consider, including availability of replacement equipment, availability of crews to install it, determinations about what equipment is considered insecure and what equipment is appropriate to replace it, and a host of other details. Creative solutions will also be called for, including customized financing and other steps to develop products and packages geared toward smaller providers, and on a longer term, the need to build American technology in software-enabled, virtualized 5G infrastructure where we can lead in safe offerings as I set out in an op-ed published in September in the San Jose Mercury News.

I have every confidence that service providers, working with the ongoing "all of government approach," will find a path forward to ensure that threats in our networks are

eliminated and that our remaining networks are secure. I consider network security to be one of my top priorities at the Commission.

Thank you again for having me here this afternoon. I look forward to continuing to work with all to ensure the security of our networks.