STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Program*, WC Docket No. 18-89

Network security is national security. As we move into a 5G world where billions of IoT devices will operate our critical infrastructure, health care system, financial sector and transportation systems via mobile wireless transmissions, secure networks are not only necessary to preserve the confidentiality and integrity of our communications, but also to protect our public safety. Today, we take an important step towards protecting these networks by prohibiting the use of universal service funds for the purchase of equipment from the Chinese telecommunications companies Huawei and ZTE. While many talk of security issues surrounding "back doors," I have said many times that the untrustworthy equipment from these companies could readily serve as a "front door" for Chinese intelligence gathering, at the expense of our privacy and national security. I fully support the effort to ban future purchases of such equipment using USF funds.

While that is necessary, it is not sufficient in addressing this issue of national security. Back in May, I published an op-ed first raising my concerns that we cannot afford to think of this issue asymmetrically, focusing strictly on prohibiting untrustworthy equipment from entering our networks, and failing to account for the reality that we already have the same equipment in our infrastructure. Lots of it. I have consistently said that the problem is real, it is here already, and our failure to address existing untrustworthy equipment leaves American citizens vulnerable to data siphoning and foreign interference. That's why I'm glad that we're issuing a Further Notice of Proposed Rulemaking seeking comment on the problem of such equipment and how to address it. As I said back in May, we need to find this untrustworthy equipment, fix the problem, and fund the remedial effort – Find It, Fix It, Fund It.

As today's item discusses, although the data collection we authorize today should provide much more information, our record in this proceeding to date suggests that much of the Huawei and ZTE equipment in our networks is held by certain rural wireless carriers. Since I first spoke on this issue, I've traveled the country and personally met with nearly two dozen of these carriers and their representatives. I held a workshop this summer at the Commission where I heard from rural carriers, equipment manufacturers, national security experts, academics, and various other stakeholders. A few weeks ago, I met with the Department of Homeland Security and the Chamber of Commerce in Denver to discuss these issues with rural carriers. And just yesterday, I published a white paper summarizing the facts, feedback and recommendations that came from those meetings.

Here's what I've learned. These carriers are made up of hard-working men and women that serve hard-to-reach communities that the major carriers can't or won't serve, operating with small teams and tight budgets. And they're worried. They're concerned that they'll be punished for using Chinese equipment in their networks that they bought lawfully and in good faith, in many cases before the full strength of our concerns about network vulnerabilities linked to Chinese telecom manufacturing surfaced. They now understand the significant security risks associated with their Chinese network equipment and software updates. They understand how manufacturers are obligated under Chinese law to cooperate with the government's demands for network access. They understand how their vulnerable equipment could be used for surveillance, disruption of critical services, or cyber-attacks. And they want to fix it. But they need our help, and this FNPRM is the first step on the road to doing so.

But such assistance shouldn't come without considering how we got into this situation and how to avoid duplicating it in the future. Based on information available today, the item indicates that replacing untrustworthy equipment in our networks could cost as much as $2 billion, and the actual figure could be even more. We can't afford to do this again. That's why I proposed the addition of questions seeking comment about what factors led to the dependence of certain carriers on untrustworthy equipment and what measures the Commission could and should take to ensure that all telecommunications carriers obtain and rely on equipment only from trusted vendors. I'm particularly interested in hearing about

American-made alternatives – both hardware and software-based – to untrustworthy or insecure telecom equipment.

As our world becomes even more interconnected, the FCC has a critical role to play in protecting that security. The Commission must be proactive, not reactive, in our national security measures in order to avoid problems like untrustworthy network equipment in the future. And though we've done much, much remains to be done. Here and going forward are a few leading issues on which you will be hearing from me.

First, we need to create an FCC National Security Task Force. The Commission currently reviews national security issues on a distributed basis among the various bureaus. For example, the International Bureau refers applications for Section 214 licenses involving foreign ownership to "Team Telecom" for national security review. The Public Safety and Homeland Security Bureau participates in the National Security Council's NSPM-4 process. And the Wireline Competition and Wireless Telecommunications Bureaus consider national security in license transfers and number portability matters. It remains to be seen which bureau will administer the tremendous task that we vote on here today in setting policy to handle untrustworthy foreign equipment.

This distributed structure makes internal coordination challenging and risks inconsistent treatment of national security issues between different bureaus. These issues are not going to diminish. Quite the opposite, in fact, as I expect that the Commission will continue to see an increase in the number and complexity of issues that will touch on national security. Security issues surrounding Team Telecom, CFIUS, 214 licensing, numbering and so forth are becoming more common. We must be more intentional than ever to ensure that the whole of the FCC is more coordinated, more deliberative, and more collaborative. The FCC should issue a Public Notice creating a National Security Task Force, like other task forces established by the FCC in the past. I look forward to discussing this idea with my colleagues.

Second, as I recently wrote in the San Jose Mercury News, we must seize this opportunity to encourage the growth of American technology for next generation networks. We cannot entrust the technological solutions to the challenges of 5G to geopolitical rivals. Rather, we must support American innovation to meet these challenges. American ingenuity has historically dominated the research, development and deployment of telecommunications technology. This must continue for 5G, and American companies are already developing alternatives to traditional telecom equipment infrastructure through software-enabled 5G and virtualized radio access networks for cloud-based 5G. 5G infrastructure development must represent the next frontier of American technological leadership.

American 5G equipment will be safer because we can be confident about it observing best practices and protecting our intellectual property and privacy from foreign actors. Most importantly, American companies do not answer to the directives of adversary states with no clear rule of law. Moreover, while artificially low prices may have provided a temporary advantage to Huawei and ZTE, I believe that the telecom industry has come to realize that the cost and inconvenience of fixing and replacing untrustworthy equipment far outweighs any short-term savings. I believe America can rise to the challenge and ultimately come out of this situation more advanced, more secure and more prosperous.

Third, our network security depends on the equipment that carries our communications traffic, and critically in some instances also on traffic that leaves our domestic networks. Like many countries around the world, the United States relies on submarine cables to carry its traffic across the oceans. Pending before the Commission now is an undersea cable application from US companies that have partnered with Dr. Peng Telecom & Media Company, one of the largest telecommunications conglomerates in China, for a cable running between Los Angeles and Hong Kong. The project is designed to carry a large portion of the communications between the U.S. and Asia, and a recent Wall Street Journal report indicated that the Justice Department has expressed concerns that the communications could be stolen, blocked, or modified on the Hong Kong end. I share these concerns as an initial matter and want to learn more about what measures can be done, if any, to prevent the Chinese government from eavesdropping, blocking or tampering with these communications.

Finally, the nation's first primaries will take place in a few months. With that in mind, I've been focused on the security of our election system. The threat is real – our intelligence agencies have confirmed that foreign actors sought to tamper with our election systems in 2016 and predict that they will try again in 2020. And while much of the media attention has centered on the use of social media to confuse and polarize us, our networks are also under attack. According to our intelligence agencies, Russian-affiliated cyber actors targeted all 50 state election systems during the 2016 voting cycle, including attacks on voting-related websites and voter registration databases. Although they weren't able to change individual votes or vote totals, we should expect another round of attempts in 2020.

That's one reason why our network security is so important. While completely disconnected voting machines are the most secure, research shows that some states still use the same networks to transmit their voting results that we use for our mobile phones. Indeed, the Federal Election Commission estimates that more than 1,000 of these machines remain in use in states like Wisconsin and Florida.

Once a device is connected to a wireless network, it's subject to the same threats as other wireless communications. Voting results can be blocked or altered by criminals or adversary states using IMSI catchers or by hacking untrustworthy or insecure routers. Because of these risks, I've reached out to the major wireless carriers to discuss how they're protecting their network security and working with election officials. The FCC has a statutory obligation to protect the national defense – the security of our elections clearly qualifies in my mind.

Moving forward, the Commission's policies must reflect the new telecom landscape. The recent influx of new, unfamiliar actors into the telecom space has rendered the old system of operations, built upon trust and familiarity, quaint. I will do everything in my power to keep Americans secure now and in the future. Thank you to my colleagues for their support of my edits to this item and thank you to the Wireline Competition Bureau and the other Commission staff who worked on this item for your excellent work.