STATEMENT OF
COMMISSIONER GEOFFREY STARKS

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

Network security is national security. As we confront foreign cyberthreats to our economy, our elections, and even our response to the COVID-19 pandemic, these words have never been truer. Certain foreign telecommunications equipment companies rapidly vaulted themselves into a leading global position, as well as a foothold in U.S. networks. Today's decision is another step by this Commission toward eliminating untrustworthy equipment in our networks. But we need a broader, more cohesive plan to develop and support alternatives that both replace existing equipment and position us to better compete in the future.

Through its "Made in China 2025" strategy, the Chinese government has provided critical support to Huawei and ZTE that artificially lowered their prices, assisted in their research and product development, and undercut international competition. This was not free-market competition, but part of a strategy to leverage economic power into geopolitical dominance. Through this unfair advantage, the equipment produced by these corporations has become pervasive around the world. At first glance, these actions could be considered simple economic gamesmanship—a tactical ploy to become the dominant telecom equipment ecosystem, set manufacturing standards, and "win" the race to 5G.

But as we've established in this proceeding, such a view overlooks the other half of the bargain between these foreign competitors and their government. According to our intelligence agencies, in exchange for this subsidization, corporations like Huawei and ZTE have siphoned data, allowed backdoor access to state agencies, and enabled functionality for network disruption. As a result, the technological foundation of our communications networks has been weaponized.

But the tide is turning, as evidenced by this week's decision by the UK government to ban Huawei from its 5G networks. Here in the United States, last year I called for the FCC to find each piece of untrustworthy equipment in our networks, to fix the problem by instituting a replacement program, and to fund the replacement of this equipment. My find it, fix it, fund it proposal was a comprehensive and unequivocal response—untrustworthy equipment that threatens our data privacy and network security cannot be managed or tolerated in any form.

Today, we largely codify that response and integrate it with the provisions of the Secure and Trusted Communications Networks Act. Universal Service funds will no longer be used to finance commerce with bad-faith actors, and we begin proceedings to replace the untrustworthy equipment in our networks.

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 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. A few additional thoughts.

First, as I've called for before, 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 authorizations 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.

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 authorizations, 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.

Second, as we proceed, we must promote equipment supplier diversity and level the competitive playing field so we have options for replacing this equipment and avoid replicating this situation in the future. We must also champion new innovations that can ensure a more robust, reliable communications network. This includes serious consideration of Open RAN (O-RAN) technology solutions for replacing untrustworthy equipment and updating our communications infrastructure more generally.

O-RAN is promising because it enables a single distributed system of interoperable hardware. With interoperability, individual components can be interchanged without replacing whole systems. This granular approach reduces the barriers to entry for radio access network component vendors, particularly small-scale or specialized suppliers, and presents an opportunity for American companies to reassert their role in the communications equipment sector. A new competitive and diverse market of vendors would allow each carrier to establish the most innovative and appropriate combination of network components for its needs, rather than purchasing equipment on a one-size-fits-all basis.

O-RAN emphasizes software defined functions through open interfaces and a cloud hierarchy. Both features accommodate innovation and allow for a more robust and responsive network environment. For example, scaled design improvements, as well as updates to network systems, may occur at lower costs and faster timetables. This responsiveness will allow carriers to harmoniously merge legacy and next generation wireless systems as they replace older or untrustworthy equipment.

And we know that O-RAN isn't—as some have suggested—"pie in the sky." It is available right now. DISH Network recently selected network software provider Mavenir to deliver cloud-native O-RAN software to buildout its 5G wireless networks.

The scope of our item today focuses on how we "rip" and not on how we "replace." But in reality, the two go together, by necessity. We must do some deep and proactive thinking on the best policies to effectuate our goals of promoting secure telecommunications networks that benefit our shared future and get the best value for American tax-payer dollars. So here's a new idea. In future items, I recommend we explore that each "rip-and-replace" carrier rebuilding its network be required to consider solutions offered by an O-RAN provider. That would achieve many of our goals, including encouraging global competition with Huawei, capitalizing on U.S. software advantages, accelerating the development of O-RAN as a product-model and a business-case, and allowing for alternative vendors to enter the market and offer specific network solutions. If American tax-payer dollars are going to rebuild these networks, Americans should get the best value and the most benefit.

Third, even as we discuss potential alternatives to the untrustworthy equipment in our communications networks, we still lack the funding necessary to remove and replace that equipment. Last year, in meetings across the country, small carriers repeatedly told me about their need for help to replace equipment that they bought legally and in good faith. To their credit, many of these same carriers have experienced substantial losses as a result of honoring the Keep Americans Connected Pledge, further weakening their ability to replace this equipment on their own. We must coordinate with Congress to ensure that sufficient funds are appropriated, and that a remedy can be provided quickly and responsibly.

Our actions today are swift and clear, but much work lies ahead. We must join with policymakers both here and abroad to address not only the challenge of untrustworthy equipment already in our networks but how to respond to adversary states' attempts to leverage market dominance into geopolitical influence. Experience has taught us that we can counter these efforts only by identifying a realistic alternative. Let's get to work.

Thank you to the staff of the Wireline Competition Bureau for their work on this item.