REMARKS OF COMMISSIONER GEOFFREY STARKS
AT THE FCC & NCSC NATIONAL SUPPLY CHAIN INTEGRITY JOINT WORKSHOP

APRIL 26, 2021

Thank you and good afternoon everyone. Today we gather during National Supply Chain Integrity Month to discuss ways to strengthen our supply chain against potential bad actors. Over the past decade, our networks have faced a rising tide of activity by adversary states and others intent on compromising Americans' privacy and security. As we seek to enhance our networks to support innovative technologies, policymakers, industry and consumers must ensure that those networks are sufficiently fortified to preserve the critical economic, privacy, and security interests at stake.

The FCC has a vital role to play. Congress explicitly created our agency "for the purpose of the national defense" and "for promoting safety of life and property through the use of wire and radio communications." Some have indicated that FCC has a limited role in this space -- overseeing the makeup of communications networks, focusing on potential radiofrequency interference and other technical issues. But the complexity of protecting the American public and the fundamental inter-connectedness of security issues, along with long-term economic and international trends, including the disappearance of the American telecom hardware sector and the growing role of Chinese vendors, have compelled the FCC to embrace its role. Network security is national security. Thus, in 2019 we prohibited the use of universal service funding to purchase or support equipment or services posing a national security threat. That year, I challenged the Commission to begin the process of finding the untrustworthy equipment already in our networks, setting out a plan to fix it, and funding the replacement process. A year later, we determined Huawei and ZTE posed significant risks to national security, collected data on their presence in U.S. networks, and strategized a reimbursement plan to cover the cost of replacing the equipment, which could be close to $2 billion.

This experience underlines the point that smaller companies often are at greatest risk for supply chain issues. I've spoken to many rural wireless carriers about how they came to purchase Huawei and ZTE equipment in the first place. While they did so legally and in good faith, concerns about this equipment aren't exactly new. Nearly 10 years ago, a bipartisan report from the House Intelligence Committee observed the national security threat posed by Huawei and ZTE and advised that American companies should avoid buying their equipment. But small carriers purchased this equipment because they felt they had no other choice. These carriers, which serve many parts of the country that would otherwise be left unserved, are often family-owned small businesses operating under significant financial pressure. As such, the smaller carriers told me that they lacked the bargaining power to negotiate bulk discounts or customization with the large equipment vendors. Thus, they were willing to listen when Huawei and ZTE offered seemingly high-quality equipment at competitive prices.

My takeaway from these conversations is that barring Huawei and ZTE from our networks is only part of the solution. No one forced these carriers to purchase Chinese equipment – they did so because they believed, right or wrong, that they didn't have any better options. Policymakers must ensure that small and mid-sized carriers have access to equipment and services that are not only secure but make good business sense. That's why I'm glad that the Commission has included Open Radio Access Network equipment and services as an option for carriers participating in our replacement program.

Open RAN is a new telecom infrastructure model that promises to increase efficiency and security while promoting American leadership. Rather than being tied to the proprietary system of a single vendor for its entire network, a carrier using Open RAN can build its network out of vendor-neutral hardware that performs network functions using software-defined technology. This will allow carriers to make upgrades, including adding 5G capabilities and new spectrum bands, via software updates instead of hardware replacements, which can be expensive and time-consuming, particularly in the remote areas often served by small and mid-sized carriers.

By its nature, Open RAN also addresses a recurring network security problem -- the lack of transparency. Traditional closed network systems can have security flaws that don't become known because they involve only a single vendor that may keep that information non-public. In contrast, because Open RAN necessarily involves multiple vendors, security problems can be identified and resolved more rapidly than in traditional networks. As the saying goes, "sunlight is the best disinfectant."

Moreover, American companies like Altiostar, Mavenir and Parallel Wireless are leading the way on Open RAN around the world. America has long been a leader in software development, and many US companies are stepping up to provide software for use in Open RAN networks in North America, Asia and Europe. Open RAN could be a huge opportunity for American businesses.

But among all this optimism, questions remain. Rural carriers have told me that they're interested in Open RAN, but are worried about whether it's going to work. These aren't large carriers that can afford to experiment, particularly with federal dollars. Open RAN companies need to work with these carriers to show them how to shift from their legacy network equipment to Open RAN without disrupting service. These carriers also need help from experienced systems integrators who can work with vendors to set up the network and troubleshoot any problems.

And while Open RAN could help address our network security issues, security needs to be part of the initial development of Open RAN rather than an afterthought. As another saying goes, these features must be "baked in rather than bolted on." It's critical that Open RAN vendors participate in organizations like 3GPP so security protocols become standard. This is particularly important given that a single network may now have equipment and software from

multiple vendors. The supply chain for American Open RAN networks must exclude any untrustworthy entities.

Although the Commission's efforts to promote supply chain security have focused on network infrastructure, our networks also include billions of end user devices. As the Internet of Things flourishes and connects a variety of devices to our networks, we must ensure that those devices and the Americans who use them are protected from cyber-threats.

According to one study, we will have more than 25 billion connected devices worldwide by 2025. Networks of IoT devices will help reduce carbon emissions and waste, increase productivity, protect public safety, and generally enhance our way of life. But many of these devices or their components come with exploitable security vulnerabilities. This same inexpensive equipment is most likely to be used by small businesses and consumers. One 2017 study reported that nearly half of all companies that use IoT devices have lost revenue due to a security breach, at a cost of more than 13 percent of revenue for companies with annual revenues under $5 million.

News reports have highlighted security issues regarding devices like web cameras, wireless routers, and WiFi extenders. Each device could be a potential entry point for a hostile actor to attack connecting networks, including those belonging to critical infrastructure industries, governments, and health care facilities. Late last year, for example, a technology news site found suspicious backdoors in affordable Chinese-made internet routers and Wi-Fi extenders sold at several major retailers that would allow an attacker to remotely control not only the devices, but also any devices connected to the same network. Further testing showed that these backdoors were not only potential threats, but that third parties were actively attempting to exploit them.

And while industry, Congress, and other federal agencies like NIST are highlighting the importance of securing these devices, none of these actions address the devices manufactured overseas that are likely to ignore any voluntary protections. The Commission should work with other policymakers and retailers to ensure that all devices imported into the United States and connected to our networks meet NIST cybersecurity standards. We also must develop proactive safeguards to educate users and prevent future intrusions on our IoT networks.

Finally, as with network infrastructure equipment, we must also build American leadership in this space. There is a bipartisan consensus that we can no longer afford to outsource our technological solutions. We must commit to supporting innovation by domestic companies to build a more advanced and secure future. Failing to do so risks harm not only to the consumers and businesses with insecure devices but to our broader networks as a whole.

Our supply chains should provide high-quality, secure communications equipment. I look forward to working with my colleagues and other policymakers to promote domestic solutions and security methods that ensure our networks are safe for years to come. Even as we

work to provide all Americans with next generation broadband, we must ensure that those networks are secure.