REMARKS OF
COMMISSIONER GEOFFREY STARKS
COMPETITIVE CARRIERS ASSOCIATION ANNUAL CONVENTION
PROVIDENCE, RHODE ISLAND
SEPTEMBER 17, 2019

Thank you, Steve, for the introduction and good afternoon everyone. Thank you for inviting me today – I'm delighted to be here and to learn how rural and regional carriers help to connect Americans around the country. In fact, I just came from a meeting with some of your members to talk about the issues you're facing today.

It's hard to believe that wireless service was once viewed as a luxury that only the wealthiest Americans could afford. In fact, it wasn't that long ago that a lot of people only used their cell phone for emergencies. Over the last couple decades, however, technological advances have changed wireless service from a pricey landline alternative to the connection of choice for more than half of Americans. And in that time, wireless service has shifted for many people from an exclusively voice service to one that is all about data. Whether it's using mapping applications, streaming content or any of the other amazing apps that have debuted in the last few years, mobile wireless has revolutionized our lives.

And the next generation of wireless service promises even more. As carriers continue to upgrade their 4G service and many begin providing 5G, our lives are going to change. We are already hearing about all the amazing things that will flow from the fast speeds, high capacity and low latency promised by this new technology – virtual and augmented reality, massive Internet of Things systems, self-driving cars, the list goes on and on. But what's even more exciting is to consider the unexpected. When 4G rolled out, not many people predicted the rise of the ride sharing app and the disruption of the taxicab industry. We can expect similar surprises as 5G and other advanced wireless services spread throughout the country.

It's important that all communities have the opportunity to benefit from these advancements, and I want to express my appreciation for the work performed by rural and regional carriers in addressing the issue of the digital divide. Many of you serve some of the most rural and remote parts of the country – in some cases, you may be the only carrier in the area. Bringing broadband to all Americans is an essential part of your mission.

You can see that commitment in the work performed by CCA members. For example, I visited New Mexico last month and saw firsthand the difficulties experienced by many Native American reservations in obtaining high-quality broadband service. In fact, nearly 80 percent of Tribal members living in rural New Mexico can't access the internet from home. To help address this problem, CCA Member NTUA Wireless, which is a Navajo-owned carrier, partnered with a local school district to deploy a pilot program to offer Wi-Fi connectivity on school buses. Many Native American kids in rural New Mexico have long bus rides between home and school. Students can now use that time on the bus to complete their homework and continue their education.

Another major issue facing rural Americans is the lack of access to healthcare. The Department of Health and Human Services reports that 76 million Americans live in an area with a shortage of primary care providers. That's why I was pleased to hear about C Spire's partnership with the University of Mississippi. The pilot program allows for remote monitoring

and insulin testing of diabetes patients. The program has had amazing results with ensuring that patients take their medication as prescribed and show up for their examinations. It's also saved money – with just 100 patients over six months, the program saved nearly $340,000, and experts estimate that a state-wide program could save nearly $200 million per year in hospital costs alone even if it only impacted 20 percent of diabetes patients state-wide.

Both programs sound extremely promising, and I salute the hard work of these carriers in making them a success. I look forward to watching their progress. As these stories illustrate, high-quality, affordable broadband service is essential to ensuring full participation in our economy, our education system and our democracy. That's why we should do everything possible to ensure that all Americans can receive such service.

But while I am laser focused on ensuring that service is provided to all, I also believe it's critical not to neglect the security of the underlying networks. Every part of our nation's critical infrastructure relies on interconnected telecom networks. Congress has directed the Commission to protect the national defense and the safety of life and property. That's why, as we move into a 5G world, we must recognize the changing nature of our telecom network security needs. As I have said before, Network Security is National Security.

And what are the stakes of 5G security? They couldn't be higher. One of 5G's major advantages is its ability to connect far more devices than prior standards. Governments and businesses plan to take advantage of that capability through massive Internet of Things projects. Billions of devices will connect to 5G networks to handle communications governing our energy grid, our smart cities, our hospitals, our financial system, and our transportation system.

To its credit, 5G technology removes many earlier vulnerabilities and increases the flexibility, security and reliability of the network overall. For example, segmenting operations using network slicing will allow carriers to contain attacks to a localized area and respond directly to the affected operations. And shifting network functions to software will allow carriers to prepare and deploy security updates more rapidly.

But these networks are vulnerable. Networks are defined by their interconnection with other networks, and that inherently creates risk, as the telecom "neighborhood" transforms from a small group of familiar carriers to a vast landscape of service providers, many of whom are strangers to each other.

This change has brought tremendous benefits to consumers in the form of new competition and new services. However, it has also rendered obsolete the historic presumption that every interconnected party is a good-faith actor with similar levels of security. Instead, we read story after story about bad actors – whether criminals or adversary states – exploiting gaps in our security systems to steal money or information, sabotage systems, or lay the groundwork for future misconduct.

Many of you may recall the 2017 NotPetya cyberattack, which our intelligence agencies tell us was launched by Russian state actors. What began as an attack on Ukrainian banking and critical infrastructure interests quickly spread throughout the world, infecting and effectively rendering useless computers and networks at companies as diverse as FedEx, the shipping company Maersk, and the pharmaceutical giant Merck. Unlike many other cyberattacks, this one wasn't about money – and there was no way to fix the problem. This attack was just to inflict as

much pain as possible, as widely as possible, as quickly as possible. Our government estimates that the attack inflicted $10 billion in damages worldwide.

Similar attacks happen every day. Over the last couple years, bad actors have staged ransomware attacks on cities around the country, including Los Angeles, Newark, San Diego, Atlanta and Baltimore. Hackers have locked city employees out of systems ranging from court systems, to transportation databases, to library and public safety operations. Just in the last month, 22 Texas cities and towns suffered a coordinated ransomware attack that locked city employees out of email, computer, and phone systems. These attacks force officials to make the terrible choice between paying a ransom to get their data back and encouraging future attacks, or incurring the tremendous cost and delay of rebuilding their networks from scratch.

While these are examples of hackers targeting software vulnerabilities in company or government networks, similar threats exist to our telecommunications networks. Intelligence agencies are particularly concerned about China, which has a track record of using espionage to advance its commercial and national security interests. Earlier this year, I joined my colleagues to reject an application from China Mobile to operate in the United States. While China Mobile is not officially a state-controlled company, key executive branch agencies – known as "Team Telecom" – convincingly argued to the FCC that the company could be subject to undue influence by the Chinese intelligence services. This would present a major threat to our national security, because if its application had been approved, China Mobile would have been able to connect to the U.S. telecom network and gain enhanced access to our telephone lines, fiber-optic cable, cellular networks and communications satellites. In fact, if it offered the least costly path to carry traffic on a particular route, China Mobile could have even carried the communications of U.S. government agencies. The Commission is now reviewing the existing authorizations of two other Chinese telecom carriers – and I wholeheartedly agree with the bi-partisan calls just yesterday that we need to figure out whether they present the same type of threat and act soon.

Nor are these types of concerns limited to carriers. A recent Wall Street Journal story reported on discussions within Team Telecom regarding an application pending before the FCC for an undersea cable project to connect 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. According to the story, 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 members of the group about their recommendation to the FCC. As the story notes, Team Telecom is still reviewing this project. For my part, I'm gathering information about the application and will decide my position once I have assessed the relevant record, including any recommendation from Team Telecom, to determine whether the proposed outcome protects the national defense and the safety of life and property – which is the FCC's statutory direction in this area. But you will be hearing from me on this – where there are national security issues raised with regard to our networks, I am going to pay close attention, and use my voice to make sure that we are doing everything in our power to keep Americans secure.

But the threat isn't just interconnection with untrustworthy parties. Because of the changing nature of telecom equipment, even trusted actors may have security problems that can compromise interconnected networks. For example, most legacy networks contain large amounts of interconnected hardware. But we are rapidly moving to an era where software will perform many of the functions that used to be done by these devices. This will increase the

speed and flexibility of our networks, but it will also create a new opening for bad actors. Even if the software is safe as installed, security patches could create new vulnerabilities in areas previously thought to be safe.

That's exactly what's behind the current uproar over equipment made by certain Chinese manufacturers, including Huawei. Huawei is one of the biggest telecom equipment manufacturers in the world, and although its share of the U.S. telecom market is relatively small, some wireless carriers have purchased Huawei equipment for their networks. These carriers bought this equipment, often a decade or more ago, because it was far less expensive than other options, and because Huawei was willing to work with them to create customized networks. These purchases did not violate any rules or laws.

Notwithstanding these facts, experts say that the equipment made by Huawei and other Chinese manufacturers presents serious security vulnerabilities. According to these experts, Huawei software does not have the same consistency from installation to installation as its competitors. Programming variations make it difficult or impossible even for Huawei to know exactly what software is deployed in a given build and whether the equipment will accept software updates.

Security experts tell us that this "bugginess" in Huawei software means that it has "front doors" accessible by both the company and by bad actors familiar with exploiting inconsistencies and flaws in Huawei code. Moreover, it's not just the original software that's concerning – Huawei systems are typically managed remotely with updates delivered from China. Many networks and network components get software updates as frequently as every week. Control over software updates and their delivery essentially amounts to control over an entire network.

It's because of concerns like this that the federal government is seeking to stop the importation and installation of equipment from Huawei and other Chinese manufacturers. The Commission is currently examining whether to ban the use of federal support dollars for the purchase of such equipment, but we can't ignore the problem of the equipment that's already here.

That's why I've launched my own effort to understand and address this issue. I refer to my program as "Find it, Fix it, Fund it," and this summer I conducted a workshop where I heard from carriers, academics and other security experts about this problem. These listening sessions – which included CCA and its members – were incredibly helpful in providing context to the issue and informing my approach. Here are a few lessons I drew from the discussions.

The first part of my program is to <u>find</u> the suspect equipment. Carriers told me that they are worried about being labeled as security threats, particularly when they acted legally and in good faith. That's why the Commission needs to consider a mix of incentives and regulatory action to identify where this equipment lies. In the short term, we could provide financial incentives for carriers to self-identify, but our national security may ultimately require us to direct carriers and manufacturers themselves to disclose this information.

<u>Fixing</u> the security problem is the second part of my program. Panelists at the Workshop noted that any plan for a "fix" must first define the solution to the problem. Do we need to remove all suspect equipment with a "rip and replace" approach, or can we somehow quarantine some equipment in certain parts of the network? While I am open to considering such mitigation measures as an initial approach, the long-term security of our networks will likely require

complete removal of all equipment from suspect manufacturers. Nokia and Ericsson have said that they are willing to create products and financing options geared toward smaller carriers that need to replace Chinese equipment. They also claim that they have had handled similar replacement efforts with minimal customer disruption.

I appreciate these offers, but I believe that there is a real security need for U.S. innovation in the 5G space. Last week I published an op-ed in the San Jose Mercury News advocating the use and development of domestic products like software-enabled, virtualized 5G infrastructure that could replace suspect equipment. America has long been a technology leader in software and wireless technology – growing our capability to make secure infrastructure makes sense from both a security and economic standpoint. We need to invest in research and development so we can lead in this area and not have to rely on foreign manufacturers for our security.

The final part of my program is to fund the equipment replacement effort. This is a national problem that deserves a national solution, and we shouldn't expect small carriers – who acted legally and in good faith – to replace their insecure equipment on their own. As I heard from carriers at the Workshop and earlier today, many of the carriers who purchased this equipment operate on tight margins in rural areas and may not be able to cover the costs of replacement without financial support.

I believe this problem will ultimately require congressional action. According to panelists at my workshop, a "rip and replace" program could cost anywhere from hundreds of millions to over a billion dollars. These costs also depend on the speed of any program – if we stretch out the timeline for replacement of the insecure equipment, we could save millions as equipment simply ages out of service. We must weigh this potential savings, however, against the possible risk to our national security while this equipment remains in place. Moreover, any funding should require recipients to observe good cybersecurity practices in the future. The entire federal government needs to work together as a team to see that this gets done and gets done right.

While the issue of insecure equipment has received most of the attention lately, we shouldn't forget about other threats that might originate on our neighbors' networks, even when they are acting in good faith. First, many carriers and consumers still use pre-4G technology with serious security problems. For example, these networks use a signaling protocol to transfer service data called SS7, which has well-documented security flaws that could allow an attacker to eavesdrop on calls or intercept text messages. We should encourage carriers and customers with pre-4G services to upgrade to 4G as soon as possible, while being sensitive to the needs of the often rural and low-income customers that continue to rely on these services.

But we shouldn't pretend that 4G and 5G networks are foolproof. The best lock in the world won't help if you leave your door open. And as we learned with the implementation of 4G, too many carriers fail to use available security tools or observe best practices. For example, 4G features Diameter, a more secure signaling protocol to replace SS7. Diameter uses encrypted transmissions. Unfortunately, too many operators fail to take advantage of Diameter's encryption capability even when exchanging traffic with other service providers. One study found that many operators are simply unaware of existing security issues and were failing to adopt well-publicized measures to address those vulnerabilities. The Commission and industry need to do a better job of publicizing security issues and pressuring carriers to follow best practices. Where parties continue to fall short, we should consider rulemaking.

Finally, as noted earlier, next-generation networks will connect billions of IoT devices. Each of those devices could be an entry point for a hostile actor to attack connecting networks. For example, in the infamous Mirai attack from 2016, hackers exploited vulnerabilities in multiple internet-connected devices like surveillance cameras and DVRs to launch coordinated DDoS attacks on web hosting service providers and journalists. This attack didn't even require a lot of sophistication, as the hackers simply used tools that were widely available on the internet.

More than three years later, many devices remain vulnerable to such exploits, and the Mirai-based attacks continue. Earlier this year, for example, hackers used a variation of the Mirai virus not only to attack the usual cameras and routers, but even enterprise-based IoT devices like high-capacity, enterprise-class wireless controllers, digital signage systems, and wireless presentation systems. Experts predict it won't be long before hackers target the massive industrial IoT networks that 5G will make commonplace.

While industry has done some good work in this area, the federal government has yet to establish minimum cybersecurity standards for IoT devices. As a result, although devices made by well-known manufacturers may comply with best practices, many more devices from less high-profile companies have few, if any, cybersecurity protections. And although Congress has expressed bipartisan support for action here, no legislation has been passed. The FCC needs to step into the breach before it's too late. We are already examining and certifying these devices for compliance with our interference standards. We should work with the National Institute of Standards and Technology to develop cybersecurity standards and apply them in that certification review. Once we've done so, we should work with Customs and Border Protection to prevent equipment that doesn't comply with those standards from coming into the country.

The next generation of wireless service will bring advances that we can't even imagine, and the Commission has an important role to play in terms of ensuring that all Americans can take advantage of these opportunities. But we must couple our enthusiasm for these new services with a commitment to securing our networks. Only then will we have achieved a full 5G "victory" for the American people.