REMARKS OF
COMMISSIONER GEOFFREY STARKS
"ADDRESSING SECURITY VULNERABILITIES IN OUR NETWORKS:
FIND IT, FIX IT, FUND IT"
FEDERAL COMMUNICATIONS BAR ASSOCIATION
WASHINGTON, DC
JUNE 19, 2019

Good afternoon everyone. Thank you very much for that kind introduction. I'd like to extend my congratulations to all of the award recipients that are being recognized today, including one of my own interns, Brylan Droddy, and my sincere thanks to all of you—FCBA members—for your support that makes the FCBA's Law School Scholarship and Summer Internship Stipend programs possible. These programs provide invaluable opportunities that bring new energy and perspectives into government service in communications law.

I'm Geoffrey Starks and I'm the newest Commissioner on the Federal Communications Commission. I've been a Commissioner for a little over four months now. I've hit the ground running on the many issues where the Commission has the power to make a difference, and I'm excited to spend some time with you today sharing some thoughts on one of my top priorities—the importance of securing our communications networks.

We live in a nation that runs on networks. They are vital to our way of life and enable our country's financial systems, healthcare, manufacturing, agriculture, defense, and every other part of our economy. Looking ahead, as 5G and the Internet of Things emerge, and as more and more cars, appliances, and other devices are connected, the importance of our networks will only continue to grow.

The security environment of today is very different from what we had before the '96 Act, when our communications networks consisted of a limited number of well-established carriers interconnecting with each other. Network security in those days was primarily based on simple trust, not unlike neighbors in a small town leaving their back doors open. All the players knew each other so there wasn't much risk of anyone acting maliciously.

As communications technology has evolved and new parties have entered the network, however, our telecom "neighborhood" has become more dangerous. While most carriers abide by the high security standards followed by the original small group of "trusted" entities, our original low-security environment now appears more nostalgic than practical. Bad actors now have ready access to network credentials that were once limited to trusted entities. Unfortunately, for all the promise and opportunity presented by our current communications networks, they also come with security threats.

I'm particularly concerned about the threat posed by insecure equipment in our networks. These threats don't just affect individuals or businesses—they go to the fundamental notion of protecting our nation. Network Security is National Security, and our interconnected networks are only as secure as their most vulnerable pieces. The risks of having insecure equipment in our networks are alarming—beyond the threat of foreign surveillance and hacking, there is a real risk of disruption to our communications capabilities in the event of a national emergency. In addition, these risks also mean that our critical infrastructure, financial systems, healthcare, and transportation systems are exposed.

I'm not the only one who's concerned. The FCC, Congress, and the Administration have all taken steps to prohibit or restrict insecure equipment. At the FCC, we are currently considering whether to prohibit Universal Service Fund support for insecure telecommunications equipment from Chinese companies such as Huawei and ZTE. I also recently voted to reject an application from China Mobile to operate in the United States. If its application had been approved, China Mobile would have been able to connect to the US telecom network and gain enhanced access to our telephone lines, fiber-optic cable, cellular networks and communications satellites. If it offered the least costly path to carry traffic on a

particular route, China Mobile could have even carried the communications of US government agencies. I cast this vote because of significant concerns convincingly raised by executive agencies about Chinese government influence and equipment that could seriously compromise our national security. While this vote addressed one Chinese carrier, two others with similar ownership structures, China Telecom and China Unicom, have existing approval to operate in the U.S. We need to determine whether they present the same set of threats and we need to act if they do.

Congress has also spoken on these issues. In the 2019 National Defense Authorization Act, Congress prohibited government procurement of telecommunications equipment from certain Chinese companies, including Huawei and ZTE, that were deemed to be a threat.

Likewise, the President's recent Executive Order barred U.S. companies from buying foreign-made telecommunications equipment considered to be a national security risk. The Executive Order prohibits acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology in the U.S. where the Secretary of Commerce, in consultation with several federal agencies including the FCC, finds that the transactions in question involve companies owned or controlled by foreign adversaries and pose undue or unacceptable risks to national security. The Executive Order also directs the Department of Homeland Security, again in consultation with federal agencies including the FCC, to publish rules and regulations to implement the terms of the Executive Order. Each of these actions considers what to do about insecure equipment going forward, but none addresses a critical problem—this equipment is already in our networks. Lots of it. The threat is real, and it's already here. And we need solutions. We cannot treat this issue asymmetrically – where we focus strictly on how to keep insecure equipment with a national security risk out of our network going forward, but don't address the equipment already in our infrastructure.

That's why next week I will be convening stakeholders—including carriers, manufacturers, academics, and trade associations, to start crafting and developing a practical path forward. Specifically, I anticipate digging into what it will take to Find the insecure equipment, Fix the problem, and help Fund the process. Find it. Fix it. Fund it.

First, we need to understand the scope of the threats and risks by identifying which equipment poses a threat and where it is located. There currently exists an active debate on whether all Huawei equipment poses a threat, or whether some of it could be safe. We need to consider each part of the wireless network and the threats posed. Is the risk only in the network core of routers, servers and switches? Or is the network edge, including radios and antenna, also compromised?

The FCC needs to step up here. Congress gave us the authority to gather this information, and we need to use it. We also need to work with other federal agencies, including DHS, the Justice Department, the Department of Defense, as well as the relevant intelligence agencies, to bring as much expertise as possible to address this problem.

This will be no small task. The size of the problem is far from clear, but the White House, Congress, and the intelligence community have spoken with one voice—insecure equipment in our communications networks presents an unacceptable security risk. The software embedded in the equipment is simply too vulnerable to exploitation.

Second, where we find equipment that poses a threat, we need to fix it. That's easier said than done. We need to transition carriers away from insecure equipment as rapidly as possible. A "rip and replace" approach may be necessary; if so, we must minimize disruption to consumers. That's going to take planning and time, which is why we need to start as soon as possible to restore the security of our networks.

Finally, we can't expect carriers to replace insecure equipment alone. This is a national problem and it needs a national solution. Many of the carriers who purchased this equipment are small or operate in rural areas and may not be able to cover the costs of replacement without financial support.

It could be expensive — recent legislation would allocate $700 million to fund the problem, and one estimate claims the cost could be over a billion dollars, depending on what equipment needs to be replaced, the timing of the replacement and other variables—but we can't afford to compromise our national security. The entire federal government needs to work together as a team to see that this gets done and gets done right. Of course, funding discussions must also consider safeguards to ensure that the money goes towards securing our networks.

The clock is ticking, and it has been for some time. We need to act as quickly as practicable. If we're going to ensure the security and continued success of our communications networks, we need to deal with the insecure equipment in our networks. Find it. Fix it. Fund it.

With that, I'd like to thank the FCBA for its work and for having me here today.