COMMISSIONER SIMINGTON ADDRESSES THE RURAL WIRELESS ASSOCIATION

JUNE 28, 2022

Good afternoon, it's good to be with you all virtually. Thank you for inviting me to speak to you today about securing our country's wireless networks. I understand that a large number of your member companies are participants in the rip and replace program that the FCC is administering. I just want to say, thank you for your hard work on this program. Making sure that manufacturers controlled by hostile governments do not have a foothold in American networks is vital to our country's interests.

We got here by foolishly letting our industrial capacity diminish and by naively thinking that we could safely put high-tech systems designed and controlled by our adversaries at the heart of our country's critical infrastructure. I hope that we've learned from our mistakes and that companies took the right message from the rip and replace program, which is that the government is now keenly focused on the security of devices originating from companies controlled by certain entities like the Chinese Communist Party, and that you should think twice before buying such devices. For the government's part, I hope we keep encouraging home-grown, or at least ally-grown, technological solutions.

And I certainly hope people didn't learn the *wrong* lesson from the rip and replace program, which is that you should buy the cheapest device you can find, no matter the source, and that the US government will bail you out if it turns out to have been a bad decision. Here, I hope the government makes clear that the generosity of the rip and replace program was exceptional and that in the future, companies share some responsibility for making responsible purchasing decisions too.

I actually want to talk to you about a much harder problem today, the security of wireless devices and of spectrum. With rip-and-replace, we know the problem and we know the solution. We ban certain equipment from the US and switch to trusted vendors from friendlier countries or build it right here in the US. I don't want to downplay the magnitude of the issue or the hard work of getting the solution right, but the problem is plain and the solution is clear, albeit costly.

But it's much harder to solve cybersecurity problems that stem from unintentional flaws in software and hardware rather than intentional backdoors. Complex software and hardware are inevitably littered with bugs and design flaws, and many of those turn out to be security vulnerabilities that attackers can use to steal data, hack into systems, or take them offline.

Let's consider wireless devices in particular. The FCC has to approve every consumer device with a wireless transmitter sold in this country. Our process ensures that devices transmit only in the bands they are supposed to, no higher than the allowed power levels, and in conformance with any spectrum sharing rules. But nothing about our process ensures that a hacker can't take over the device without the consent of its owner and make the transmitter operate on the wrong frequencies and at the wrong power levels. That is, malicious attackers can hijack a device's wireless transmitter and use it as a signal jammer, as an illegal transmitter in licensed frequencies, or for other malicious purposes altogether.

I'm concerned about scenarios where a vulnerability in a common device, like a popular smart phone or smart thermostat model, allows an attacker to create a massive wireless botnet of thousands or millions of devices that can then be used to take down or degrade wireless networks and critical infrastructure. A nationwide spectrum denial of service. The design of wireless protocols and networks means that an attacker can do a lot of damage, even with only low-power transmitters, like most consumer electronics. WiFi deauthentication attacks, for example, allow a malicious actor to effectively take WiFi networks down not by jamming the airwaves with raw radiofrequency noise, but by repeatedly sending specially crafted deauthentication packets. This kind of smart jamming attack requires just a tiny fraction of the transmission power that a traditional jamming attack would.

You could imagine one way of addressing this: adopting detailed cybersecurity standards for hardware and software engineers to follow. This could include mandating certain programming languages, coding styles, code review practices, and so forth. But there's reasons to be skeptical of that kind of approach. There's no way a government regulator in this country can keep up with the rapidly evolving software engineering and security state of the art. The trade of software engineering is still too young and dynamic for heavy-handed regulation. And previous well-meaning attempts at detailed security standards have devolved into checklist compliance exercises that impose a lot of bureaucratic burdens but do little to actually improve security and are in fact often obstacles to that goal. Just ask any engineer who has worked on FIPS-compliant software.

But most importantly, the FCC isn't a generalist cybersecurity agency. We don't have the legal authority to start regulating software engineering generally and we certainly don't have the expertise. But we are tasked with protecting the availability of spectrum of the benefit of the public, and I don't think we can succeed in that mission going forward unless we address the security of wireless devices.

So my office has been working on a couple of cybersecurity proposals that help address some of these issues without trying to make the FCC into something it legally or practically can't be. We don't have much time, so I'll share just one of them with you today.

Many wireless devices, like smartphones, receive regular over-the-air software updates. These updates often include new features and fixes for previously broken functionality, but most importantly for our purposes, they also contain fixes for security vulnerabilities discovered in previous versions. While some device manufacturers have good security update practices—i.e. promptly issuing security updates for devices still within their expected lifespan—others routinely sell wireless devices with no automatic update mechanism, and even those who put such a capability in their devices often fail to release security updates in a timely manner, or stop supporting devices before consumers can reasonably be expected to have stopped using them.

So there are probably millions of wireless devices in active use in this country with unpatched vulnerabilities that can allow hackers to take control of the devices, and, in addition to stealing private data, installing ransomware, and such, turn the devices themselves into signal jammers or other disrupters of wireless systems.

Currently our rules don't explicitly require a software update mechanism, but it is questionable whether the purpose of the equipment authorization rules is being fulfilled when consumer devices with software-controlled transmitters are being put to market and then promptly abandoned by their manufacturers and retailers, not receiving security updates throughout the expected lifespan of the device.

I don't think it's too much for the government to ask, that if you sell a wireless device, you make sure you have a way of fixing any later-discovered flaws that would allow an attacker to commandeer the transmitter and use it to attack the availability of our wireless networks. You shouldn't have to support devices forever, and you shouldn't have the obligation to deliver new features, but letting security vulnerabilities linger on devices with large install bases is not an acceptable state of affairs for the security of our wireless networks.

My office is eager to engage with industry and the public on these issues. So please don't hesitate to reach out to us. We really want to hear what you have to say.

Thank you all. Enjoy the rest of the conference.