REMARKS OF COMMISSIONER NATHAN SIMINGTON
AT THE FCC & NCSC NATIONAL SUPPLY CHAIN INTEGRITY JOINT WORKSHOP

APRIL 26, 2021

I am delighted to have been asked by Deputy Chief Jordan at PSHSB to participate in this joint workshop of the FCC and the Office of the Director of National Intelligence, and I look forward to hearing everyone's proposals to make United States communications technology more secure.

It was not too long ago that Chairman Pai spearheaded several important supply chain security initiatives that included decisive action in implementing rip and replace. It was a critical step in what developed into global leadership on supply chain security, including development, for instance, of the Prague Proposals, in which the United States took a leading role in developing 5G security standards.

Of course, the proof of the pudding is in the eating; likewise, the value of standards is in the implementation. The security of our nation's network infrastructure is an issue where we cannot afford to fall behind the rest of the world. And so, I applaud this group and this effort to develop not just a good theoretical understanding of what network security looks like, but proposals for concrete action. That is what is needed.

I further applaud Acting Chairwoman Rosenworcel for her leadership on this topic. While we do not always see eye to eye, and while I maybe would have chosen different language at times, I would like to call attention to her voting statement on 2019 rip and replace report and order. In it, she laid out a bold and cohesive vision for network security with which I can find little fault beyond a peccadillo here or there. It is a topic on which I am eager to work not just with our partners outside of the Commission, including many of the agencies represented here, but within the Commission as well.

I want to draw specific attention to language that the Acting Chairwoman used: "Every device that emits radio frequency at some point passes through the FCC. If you want proof, pull out your smartphone or take a look at the back of any computer or television. You'll see an identification number from the FCC. It's a stamp of approval. It means the device complies with FCC rules and policy objectives before it is marketed or imported into the United States. This routine authorization process takes place behind the scenes. But the FCC needs to revisit this process and explore how it can be used to encourage device manufacturers to build security into new products. To do this, we could build on the National Institute of Standards and Technology draft set of security recommendations for devices in the Internet of Things. It covers everything from device identification to device configuration to data protection to access to interfaces to critical software updates. In other words, it's a great place to start—and with billions of new devices coming our way we should get going now[.]"

This is exactly right. Yes, our network infrastructure is of critical importance, and perhaps deserves a special pride of place in discussions like these. But we cannot forget connected consumer and industrial IoT devices and the physical layer security improvements that can be made there. Improvements that the Commission can take a leading role in developing and fostering. Improvements without which our nation's network infrastructure is made more vulnerable--not by some state actor, but by one small jam, spoof, or man-in-the-middle attack at a time.

You folks know better than I do the idea of a threat model. And we often implicitly, and at times explicitly, premise our security conversations on threat models that represent large, well-resourced adversaries using threat vectors with systemic implications. And why not? Those are the big risks.

But an accumulation of small vulnerabilities across billions of devices has the potential to be just as devastating to our country's network security as expensive radio appliances in macro cell towers do. Perhaps even more so. It's just that the burn is slower, and the fallout less spectacular. People are hurt a handful at a time, rather than thousands or millions all at once.

Let us be mindful of wireless device security. It's a good place for the Commission to flex its knowhow and craft sensible rules. And while our office has some thoughts on how to think about these issues, it's still early innings. Our door is open; let's talk about device security.

Thank you again, Deputy Chief Jordan, for inviting me to provide some thoughts, and to all of the participants in the working group for your dedicated work. I look forward with great interest to seeing what shakes out.