REMARKS OF ZENJI NAKAZAWA,
PUBLIC SAFETY AND CONSUMER PROTECTION ADVISOR
TO FCC CHAIRMAN AJIT PAI,
AT THE INTERNATIONAL INSTITUTE OF COMMUNICATIONS
TELECOMMUNICATIONS AND MEDIA FORUM

MIAMI, FL

MAY 25, 2018

Good morning. First, I'd like to acknowledge our moderator and my former colleague Mindel De La Torre. It's great to see that there's life after the FCC.

Thanks also to the IIC for inviting me to speak. It's a pleasure to be here, and an honor to participate in this discussion with such esteemed panelists.

This is not just any panel. It's the conference's LAST panel . . . on a Friday . . . before a holiday weekend . . . in Miami. If there is ever a time to make your remarks brief, this is it. So, I'm just going to make a few points before we begin our discussion.

First, harnessing the power of communications technology to make our communities safer is one of the FCC's highest priorities under Chairman Pai's leadership. And for good reason: public safety was spelled out as a core mission in the Commission's founding statute, which, by the way, was adopted in 1934. Think about that for a second. More than 80 years ago, our Congress had the foresight to understand that the reliability and resiliency of our communications networks was a public safety and national security issue.

The changing communications landscape has not only elevated the importance of network security, it has also created new challenges.

One of those is the integrity of the communications supply chain—that is, the process by which products and services are manufactured, distributed, sold, and ultimately integrated into our networks.

For years, U.S. government officials have expressed concern about the national security threats posed by certain foreign communications equipment providers in the communications supply chain. These risks include "the capacity to maliciously modify or steal information" and "conduct undetected espionage." In more colloquial terms, a hostile foreign power could use hidden "backdoors" in our network equipment to spy on Americans or attack critical infrastructure by launching denial-of-service attacks or unleashing viruses.

The FCC doesn't have the authority or capacity to protect the communications supply chain by itself. But we do have an important role to play.

For example, the FCC is the steward of the Universal Service Fund. Through this fund, we spend nearly $9 billion a year to help connect rural areas, low-income Americans, schools and libraries, and rural health care providers. And to put it simply, this money shouldn't be spent on equipment and services that undermine national security. That's why we've proposed a rule that would prohibit universal service support from being used to purchase or obtain any equipment or services produced or provided by any company posing a national security threat to communications networks or the communications supply chain. We are currently seeking public input on this proposal and look forward to reviewing the feedback on how it can best be implemented.

Let me shift now to emergency response. Obviously, nobody thinks of the challenge of emergencies and natural disasters as a new issue, but last year the United States was hit with a string of powerful hurricanes. And in particular, the devastation caused by Hurricanes Irma and Maria in Puerto Rico and the U.S. Virgin Islands was unlike anything we've ever seen.

In the immediate aftermath of the storms, the FCC took a series of actions to help restore communications services on the islands. For example, in addition to providing public information on network outage conditions and sending staff to monitor and aid recovery efforts, we granted more than 500 waivers and requests for Special Temporary Authority to help re-establish communications, offered carriers serving the territories nearly $77 million in advanced emergency universal service funding to assist with network restoration, expedited approval of experimental licenses for Alphabet's Project Loon to provide Internet access to residents, and granted targeted and flexible universal service support to help reconnect schools and libraries.

This March, nearly 6 months after the storms, Chairman Pai and a team of FCC employees visited both Puerto Rico and the Virgin Islands and there's still evidence of the storms' destruction everywhere: snapped telephone poles, cable lines lying on the ground, hollowed out buildings.

There is more that needs to be done to restore communications networks and strengthen them for the long haul. That's why the Commission recently voted to create two separate funds—the Uniendo a Puerto Rico Fund and the Connect USVI Fund—that will support these important tasks. In particular, these funds will provide additional short-term funding to carriers in Puerto Rico and the U.S. Virgin Islands, and the Commission is seeking comment on a proposal to provide a dedicated stream of long-term funding to expand broadband access on the islands. All in all, we are looking at directing almost $1 billion to these important objectives.

We are also asking questions about how to future-proof the territories' networks because we know that Irma and Maria won't be the last storms to hit there. Making the right calls now will help ensure that funding is fiscally responsible and enables as many people as possible in the territories to benefit from fixed and mobile communications.

Finally, I want to very quickly highlight another public safety priority for Chairman Pai. One of the most recent notable advances in emergency communications in the United States has been Wireless Emergency Alerts. Deployed in 2012, these text-like messages, which are accompanied by a noise and vibration and delivered to mobile devices, have been used over 36,000 times to warn the public of emergencies like tornadoes or wildfires. And the Commission is committed to making this good thing better.

One way we're doing that is by improving geo-targeting. We've found that if people receive alerts that do not impact them, they are more likely to disable this functionality or disregard future alerts. That becomes a real problem when a real emergency strikes their area. So earlier this year, we adopted rules to require wireless carriers to deliver alerts that more precisely match the area affected by an emergency. Late last year, national wireless carriers were required to enable alert initiators to include active URLs with alerts in order to make it easier for people to learn more about an emergency. We are also moving forward with plans to extend the length of alert messages from 90 to 360 characters and to support messages in Spanish.

I look forward to discussing these and other topics during this panel. More important, I look forward to continued engagement with everyone here on ways to improve public safety through communications technology.

Thank you.