REMARKS OF
COMMISSIONER JESSICA ROSENWORCEL
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
COMMUNICATIONS TECHNOLOGY LABORATORY INNOVATOR SERIES
GAITHERSBURG, MARYLAND
SEPTEMBER 27, 2019

Good morning. It is a treat to join you at the National Institute of Standards and Technology. It is also a privilege to be the first Commissioner from the Federal Communications Commission featured in your Communications Technology Laboratory Innovator series.

I have deep admiration for the work you do. Here at NIST you are responsible for promoting innovation by advancing measurement science and standards. You are living proof that we can make real, data-driven progress in some of the biggest issues affecting modern life. So speaking on behalf of the FCC and the rest of Washington, please tell us how you do it!

At the FCC, I've come to realize that while big policy ideas get all the glory, the technical details are often what matters most. The small decisions we make can have far-reaching economic and social consequences about who we reach with communications and how we secure digital age opportunity for all. For this reason, I think standardization efforts and the decision-making structures that surround them are attracting more attention than ever before.

This is especially true for cybersecurity.

"Rarely has something been so important and so talked about with less and less clarity and less apparent understanding." So said General Michael Hayden, the former Director of the United States Central Intelligence Agency in remarks about cybersecurity. He went on to describe how so many in Washington have been unable to pick a course of action to deal with this issue because they can't form a clear picture of the long-term legal and policy implications.

I think that's true. But here's the thing. To realize the full hope and promise of the digital age, we need to address the cyber challenges that are multiplying all around us. We need to take them head on.

To do this effectively, I think we have to demystify this realm. We need to speak about these problems in a way that is clear and compelling. In my experience, a good story can help do that. After all, a good story is universal.

So today I'd like to share three stories about cybersecurity. I think each one teaches an important lesson. But instead of just sharing these narratives, I want to accompany each one with an idea about how the FCC, sometimes with a little assist from NIST, can make progress securing our shared digital future. So three stories, three lessons, and three ideas. Here it goes.

I. First, for cybersecurity we need to treat the disease and not the symptom.

Every now and then we hear a story about cybersecurity that dominates the headlines so thoroughly that it has the effect of making all other security concerns seem small by comparison.

My first story is like that. It starts on a quiet Thursday morning late last year. If you are anything like me, you started that day with coffee, fumbling with your phone and looking for the news you might need for the day ahead.

After you moved past the weather and scrolled through the latest tweet storm, you would have stumbled on to a bombshell investigation in Bloomberg Businessweek. It read like the plot of a Tom Clancy novel. You know, the kind of thriller you pick up at the airport and read at the beach on vacation and is best accompanied by a cool drink in hand. Now according to the story, Chinese cyber spies used a United States-based firm to secretly embed tiny computer chips into devices. These devices were then purchased and used by almost thirty companies—including Amazon and Apple. On top of that, the report suggested the compromised devices were used in Department of Defense data centers, Central Intelligence Agency drone operations, and the networks of Navy warships.

The companies named in the report quickly denied it. But true or not, the story sent a shudder through Washington. It painted a picture about security that was worth a thousand words. It was better than a hundred policy papers and well-honed briefing sheets. Because it made crystal clear that supply chain security is a prerequisite for all cybersecurity.

Now in the telecommunications sector, when we talk about supply chain security, Chinese companies stand out. Namely Huawei. And much like our story, this commands attention. So much so, it has become the singular focus of our thinking about 5G wireless security. That is a mistake—our efforts need to be broader.

Of course, our attention here is legitimate. Work is underway at the Department of Commerce that would prevent the use of network equipment that could raise national security concerns. In Congress, legislation is on deck that would replace this equipment in the limited number of places where it exists today. And at the FCC we have a rulemaking to ensure that our universal service fund, which supports broadband deployment in rural areas, will not be used going forward to purchase insecure network equipment. We need to complete this rulemaking as soon as possible.

But we also need to think beyond these efforts. Because the situation with this company is just a symptom of a larger problem—and all of our activity so far is about treating the symptom, not the disease.

The disease is that there is not a broader market for secure 5G wireless equipment. If we want to make sure that no one company can undermine our national security, it's time for the United States to develop policies that help spur its creation.

The fastest way to do this may not be intuitive, but it begins with the United States making more mid-band spectrum available for 5G wireless services. To understand why requires a bit of background. 5G is the next generation of wireless service and it is poised to deliver speeds as much as 100 times greater than the current generation of wireless service, with much lower latency. It will open up a whole new range of wireless uses, connecting so much more than just smartphones by adding connectivity to many more things in our lives. Expect advances in industrial monitoring, robotics, healthcare, and more. It's a big deal. All around the world, countries are racing to lead the 5G wireless charge by rolling out networks as soon as possible.

The United States is vying for a leadership position, too. As part of this effort, the FCC has aggressively focused its early efforts to support 5G wireless service on bringing high-band spectrum, known as millimeter wave, to market. These airwaves have significant capacity, but also real propagation challenges. This sets us apart from most countries around the world, which are looking to mid-band airwaves for their 5G wireless deployments. While mid-band spectrum has less capacity than millimeter wave, its signals travel further. As a result, deployment is more feasible in more places on mid-band spectrum because fewer terrestrial facilities are required to make it work.

Here's the problem. There is only one Chinese vendor serving most mid-band airwaves. That means countries building their 5G networks using this critical spectrum do not have a competitive choice for secure equipment.

In the United States we have unique skill and scale. That means where deployment in the United States takes place, vendors follow. So it's time for us to make it a priority to make mid-band spectrum available, too. Our carriers will build there, and that means more vendors will compete to serve there. And when we expand the market for secure equipment at home, it also grows abroad.

At the same time, we need to be mindful that in a global economy, secure networks in the United States will only get us so far. Our networks will still connect to insecure equipment abroad. So the FCC should start a proceeding to investigate the best practices carriers can employ to mitigate that risk. We need to research how we build secure networks that can withstand connection to equipment vulnerabilities around the world. When we do, we should explore dedicated network segmentation, cross-layer security standards, the role of encryption, and routing validation. We could even ask our licensees how they use tools like the NIST Cybersecurity Framework—so that we can ensure that licensees have a structured way of thinking about network security and are using a common language to manage risk.

Like General Hayden suggested, if we want to make real progress, we have to look up from the immediate problem and start addressing the broader forces at play.

II. Second, we should transform the Internet of Things into the Internet of Secure Things.

My next story is about chocolate. Turns out it's not just my weakness.

As Misha Glenn tells it in his book about global crime, this story starts with a British bank. Like most institutions, this bank understood the real vulnerabilities of digital age finance. In fact, they spared no expense when it came to cybersecurity. They carefully assessed the risks of their operation and spent liberally to ensure the secure transfer of funds. And in the process, they convinced themselves that their comprehensive efforts had made them just about invincible. Of course, pride often comes just before the fall.

Despite their best efforts, it didn't take long for a hacker to find a vulnerability. It wasn't in the bank's systems for transactions, deposits, or accounts. It was in a vending machine filled with chocolate bars that was located in a room at headquarters. The vending machine had its own IP address. But the bank neglected to put it on the system for automated software patching updates. After all, when you plan for security updates, the machine where you drop your spare coins for something sweet when working late is unlikely to be the focus of your efforts. It may not even be on your list.

But that is all it took for this British bank to be penetrated. A single vending machine packed with chocolate. I think this is a sweet demonstration of how much around us is connected and how much work we need to do to make sure that what is connected is secure.

So here's the lesson. The equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks. That means focusing on network equipment and supply chain security is not enough. We also need to focus on the security of the connected things—otherwise known as the Internet of Things.

Right now the Internet of Things is headed our way in full force. By the end of the decade, globally there will be more than 20 billion connected devices in the world around us. When powered by 5G wireless services, we have extraordinary opportunity to use these lightning-fast connections to make our lives more efficient and effective. But as our connections multiply, so do our cyber vulnerabilities.

You can already see it—not just in breached vending machines with chocolate, but in efforts to breach city systems, connected cars, and critical infrastructure. The frequency of these events is only going to accelerate.

So back in February of this year, in a speech at the Center for Strategic and International Studies, I offered a brand-new idea to address the growing challenges of so many connected things. I laid out a path for transforming the Internet of Things into the Internet of Secure Things.

It goes like this. Every device that emits radiofrequency 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 process for equipment authorization takes place behind the scenes. But why not have the FCC used this equipment authorization process to encourage device manufacturers to build security into new products?

Here's the best part. We could work with NIST to do it. That's because just last month NIST released a set of draft security recommendations for devices in the Internet of Things. The guide specifies the cybersecurity features to include in network-capable devices, whether designed for the home, the hospital, or the factory floor. It's thoughtful stuff—like the work NIST does across the board. Plus, it covers so much that is essential—device identification, device configuration, data protection, access to interfaces, and critical software updates.

Once the NIST process is finished, we could take your work and use it to update the equipment authorization process at the FCC. In other words, we could use your thinking to reward those devices that comply, by expediting equipment authorization or expanding our process to include a cybersecurity certification before we offer the stamp of FCC approval on any connected device.

III. Third, we need to make cyber hygiene routine.

My last story is about what is called a candy drop. But it has nothing to do with the chocolate bars in the vending machine I spoke about earlier.

So picture a dusty parking lot just outside of a United States military base in Afghanistan. The vehicles rumble in and out, but otherwise it's actually an uneventful place. Or it was. Because about a decade ago, a foreign agency dropped a bunch of memory sticks in this parking lot. Now in preschool we are all taught not to take candy from strangers. And really, that same principle applies here. Nonetheless, one soldier happened upon a memory stick in the dirt. He picked it up and took it. Then his curiosity got the better of him. He decided he wanted to see what was on it.

So this lone soldier took an innocuous-looking memory stick with him back to the base and plugged it into his computer. That was all it took. Candy dropped, picked up and put into a device. As a result, our classified networks were penetrated by a foreign espionage agency.

This story—from the pages of WIRED—is so simple. But it makes clear that for all the complex technical work we need to do with supply chains and equipment authorization, we also have to mind the mundane.

In other words, we also need to talk about cyber hygiene. It's like washing your hands or covering your mouth when you cough. We protect ourselves, but we also have a responsibility to protect those we connect with throughout the course of the day. What is true for our physical lives also needs to be true for our digital lives.

Moreover, we have to start treating matters of cybersecurity as issues not just for lawmakers or regulators, but for all citizens. The lack of understanding about this topic is becoming a democracy problem. We need a serious public dialogue about cyber hygiene because the small choices we make in our day-to-day digital existence can have a big impact on our economic and national security.

The FCC should help with this effort. In our work, we regularly interact with consumers, organizations, and state and local officials. We need to do more outreach that touches on the basics of cyber hygiene—from downloading software upgrades for devices to assessing connection security when using unlicensed airwaves. And NIST, if you have thoughts about how to help foster a broader dialogue about cyber hygiene, please speak up. We need all good ideas—and we need them now.

So those are my stories. I hope they help make clear that we can do more at the FCC—with an occasional assist from NIST—to advance cybersecurity. I also think the point I started with from General Hayden is both correct and totally unacceptable. He suggested that while cybersecurity is "so important," Washington was stuck, unable to choose a course forward. I think we need to bring that digital age paralysis to an end. Because with issues like equipment security, vulnerabilities in the Internet of Things, and cyber hygiene, there is a way forward. Now let's work to make it happen.

Thank you.