REMARKS OF
CHAIRWOMAN JESSICA ROSENWORCEL
CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES
WASHINGTON, D.C.
JANUARY 17, 2023

Good afternoon. Thank you to the Center for Strategic and International Studies for hosting this very timely discussion. Today CSIS is releasing a new paper on the strategic imperative of United States leadership in next-generation communications networks. So I am very happy to have this opportunity to talk to you about this important topic on the heels of a major victory—the election of the United States candidate, Doreen Bogdan-Martin, as Secretary General of the International Telecommunication Union.

Now in the grand scheme of things, this was a little-known election at a little-known United Nations agency. A whole lot more ink was spilled on the midterm elections here at home. So you are forgiven if you missed this one. But Doreen's ascendance to this role matters. In fact, it really matters for the technology leadership that is the focus of today's CSIS paper.

Let me explain why. Doreen is the first woman to lead the ITU. That's something—and I know. I am the first woman confirmed to lead the Federal Communications Commission. The instinct to get things done and make up for lost time is real. She is also only the second American to lead the ITU in its history. Her now-former opponent was a Russian candidate and one-time Huawei executive. Plus, the Secretary General she replaced was a Chinese national who was in the top position at the ITU for eight years. At stake was control of the agency responsible for setting standards for emerging technologies like 5G. This is no small thing. Because those standards can support democratic values—or suppress them.

In the run-up to the vote, the *Washington Post* warned that the winner would determine whether next-generation technologies would be free and open or censored and controlled by governments. *WIRED* went as far as to say that the vote could change the course of internet history itself.

Well, the votes are in, and the global community has spoken. One-hundred-and-thirty-nine countries voted for Doreen's vision of technology that empowers individuals and strengthens communities. And only 25 countries cast their ballots for her Russian opponent.

By any measure, this is a massive victory. It shows that in the United States we are at our best when we are working with our allies and investing in our strengths: our hard-wired belief in defending freedom, championing opportunity, and respecting the rule of law.

But no rest for the weary. We now need to build on this momentum—and it is going to take work. Because there is intense competition underway to shape what comes next. And at the heart of that competition is how next-generation 5G networks are deployed and evolve.

There is good reason for this. So often when we think about 5G in the United States we talk about our phones. But if we do this right, our phones will be the least interesting thing about

our 5G future. This is not about the small icon that appears—and sometimes disappears—in the upper right-hand corner of a mobile device. It is a whole lot bigger than that. We are talking about using 5G technology to lay the foundation for digital transformation around the globe. Because we are fast heading to a world where next-generation wireless networks connect everyone and everything around us. They will open up possibilities for communications that we cannot even fully imagine today. By exponentially increasing the connections between people and things, this technology could become an input in everything we do—improving agriculture, education, healthcare, energy, transportation, and more. The data we derive from all these connections is powerful. It will inform machine learning, artificial intelligence, and the next-generation of innovation across the economy.

This is exciting. But these opportunities also reveal broader geopolitical challenges. Because, let's be honest, the United States and authoritarian regimes have different views on how to use 5G technology. The vision that succeeds in a global forum like the ITU matters. It will inform how networks are deployed and evolve around the world.

Closer to home, the deployment of these networks also involves big security challenges. Because the truth is that 5G networks connecting so much more in our lives will mean a broader attack surface for cyber events.

So today I would like to talk about how the FCC is meeting that security imperative. We are doing a lot—in fact, right now the agency is doing more to address network security than at any point in its history. It's a strategy to *deter, defend, and develop*: deter bad actors, defend against untrusted vendors, and develop a market for trustworthy innovation. By doing this, we are working to help improve communications security at home and shine as an example for the rest of the world.

That is a lofty sentiment. So let me take you back down to the ground and tell you what it looks like in the FCC day-to-day.

First up, coordination. The FCC is only one part of the cyber regulatory landscape. That means coordinating with others is vital.

In my first few weeks as Chairwoman, I made it a priority to reach out to my peers in other parts of the federal government to advance our shared interest in network security. Those efforts included speaking with leadership at NTIA, CISA, and the Deputy National Security Advisor for Cyber and Emerging Technology.

I also revitalized the Cybersecurity Forum for Independent and Executive Branch Regulators. When I took the reins at the agency, it had been all but abandoned. Now this revamped forum—which I run—brings together the leadership of 32 federal agencies to coordinate efforts. The group includes the Department of Homeland Security, Department of Health and Human Services, Securities and Exchange Commission, and the Nuclear Regulatory Commission, among others. We all have different authorizing statutes and different responsibilities, but we share a commitment to enhance the security of critical infrastructure.

After taking the reins at the agency, I also worked with the State Department to change the two-decade old process used for approving licenses for submarine cables. Our revised approach improves security coordination by better incorporating the work of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector into the license assessment process.

Finally, I updated the way the FCC reviews matters related to national security with the creation of a special team of experts from across the agency charged with advancing a comprehensive approach to securing our Nation's communications, which we call the FCC's National Security Policy Council.

Second, cooperation. Network security is not a subject the public sector can address on its own. Our adversaries are too numerous and move too fast for government to be effective by itself. Public-private partnerships are essential for effective cybersecurity and resilience. That is why last year I re-established what I think is one of the FCC's most forward-leading public-private partnerships—the Communications Security, Reliability, and Interoperability Council. But more than that, I specifically gave this new council a 5G focus, and did something that has never been done before—I designated CISA as my co-chair. In addition, in light of security breaches in the communications sector, I asked the council to review new risks to service provider operations from attacks in software and cloud service stacks and also develop mitigation strategies.

Third, information sharing. Technology will not solve the cybersecurity problem alone—we need better information sharing, too. So, working with our national security counterparts, last year I published the first-ever FCC list of communications and services that pose an unacceptable risk to national security. We call this the Covered List and we developed it using authority in the Secure and Trusted Communications Networks Act. Our initial Covered List included equipment from Chinese companies Huawei, ZTE, Hytera, Hikvision, and Dahua. Since then, we have added equipment and services from five additional entities—China Mobile, China Telecom, China Unicom, Pacific Network Corp. and its wholly owned subsidiary ComNet, as well as Kaspersky Lab. The FCC's rules prohibit the use of federal funds to purchase equipment or services on the Covered List. But the list does more than that—it provides companies making their own purchasing decisions clear signals about the security of products in the marketplace.

Fourth, network security. Equipment with known insecurities has no place in our networks. So with the help of Congress, the FCC launched a reimbursement program to finance efforts to take untrusted equipment out of our networks and replace it with secure alternatives. That means nationwide we are supporting the removal of equipment from Huawei and ZTE, both companies on the Covered List. This effort is now underway, though completion by carriers depends, in part, on further funds from Congress for the reimbursement program—and that is key. When we set up this reimbursement program, we also made clear this was an opportunity for carriers to transition to open radio access network systems. In the long run these systems can help diversify the technology in our networks and grow the market for more secure 5G equipment.

Fifth, network resilience. It is impossible to stop all cyberattacks and network outages. So we have taken steps to make sure networks can bounce back after an outage—whatever the cause. Late last year, following reports that the Nation's emergency alerting systems were susceptible to serious security vulnerabilities, we launched a rulemaking to require broadcast Emergency Alert System and Wireless Emergency Alert System participants to have a cybersecurity risk management plan and deploy the most recent security patches. In addition, we adopted new rules to improve network resiliency during disasters and launched a new inquiry on the security of internet routing. Every one of these activities is a commitment to making sure that our communications networks are there when we need them most.

Sixth, equipment security. For the first time, the FCC has adopted rules that prohibit the authorization of equipment for national security reasons. This is a big deal. Using authority under the Secure Equipment Act, the FCC will no longer authorize telecommunications or video surveillance equipment from Huawei or ZTE. In addition, the FCC will not authorize telecommunications or video surveillance equipment from Hytera, Hikvision, or Dahua that is used for the purpose of public safety, security of government facilities, physical surveillance of critical infrastructure, or other national security purposes. That means this equipment can no longer be imported into the United States or sold on our shores. Our action covers the base station equipment that goes into our networks, the phones, cameras, and Wi-Fi routers that go into our homes, and even re-branded or "white label" equipment that is developed in the marketplace.

Of course, the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks. So we also launched a new inquiry on the security of the internet of things. On top of that, I am working with colleagues across the government to explore how commercial labeling efforts can help improve security for the internet of things.

Seventh, data security. Our mobile phones are in our palms, pockets, and purses. We rarely go anywhere without them because being able to reach out anytime and virtually anywhere is so powerful. But this always-on connectivity has consequences. It means that carriers have access to a treasure trove of data about who we talk to, where we go, and who we are.

We need to make sure this deeply personal data does not fall into the wrong hands. That is why the FCC has long had rules that require carriers to protect the privacy and security of data, under Section 222 of the Communications Act. But the rules we have on the books that require carriers to notify consumers and law enforcement about data breaches are more than 15 years old. So we have started a rulemaking to bring them into the modern era. In the process we are also seeking comment on how our obligations can work alongside those forthcoming from CISA under the Cyber Incident Reporting for Critical Infrastructure Act.

Eighth, foreign ownership. At the FCC we have a long history of working to open United States markets to foreign telecommunications companies when doing so is in the public interest. These connections can make us stronger because they help share our democratic values with the rest of the world. But we also recognize not every connection is consistent with the

national security interest of the United States. When this is the case and we cannot mitigate the risk, we need to take action.

For this reason, working with our national security colleagues, we revoked the operating authorities of four Chinese state-owned carriers under Section 214 of the Communications Act. By doing this, the FCC established a clear process for taking away a foreign carrier's right to operate in the United States when there are national security concerns that cannot be mitigated. This kind of revocation had never happened before—so this precedent really matters. At the same time, we announced a first-of-its kind settlement against a company that was required to divest unvetted Russian ownership, pay a civil penalty, and put in place new security procedures to review any new ownership through the Office of Foreign Asset Control at the Treasury Department.

Ninth, support trustworthy innovation. Like I mentioned at the start, we are doing more than just deterring bad actors and defending our networks. We are also developing more opportunities for trustworthy innovation. To get this effort started, we moved fast to make more mid-band spectrum available to support commercial innovation and 5G network deployment. Now, after completing successful mid-band auctions in the 3.45 and 2.5 GHz bands, we are planning for what is next by working with Congress to reauthorize the FCC's authority to auction spectrum licenses and refresh the Nation's spectrum pipeline.

In addition, we launched the first-ever inquiry in the United States into open radio access networks. I also established two innovation zones in Boston and Raleigh for advanced wireless communications and network innovation research that can help support open radio access development. But a bigger boost is coming. Because in the CHIPS and Science Act, Congress provided $1.5 billion in support for this technology. While these funds are with our colleagues at NTIA, my hope is we can align their efforts with what we have learned in our existing reimbursement program about real-world deployment and the importance of systems integration.

That's a lot. We are making progress, as you just heard, on nine fronts. So let me round that out to neat ten and tell you what we are going to do next to keep up this momentum.

Tenth, keeping national security assessments up-to-date. We know that network security threats are always evolving. If you have listened this far, you know I believe FCC policies have to keep pace. It sounds simple, but in practice this is not always easy. This is especially true when it comes to FCC licensing, where our practice has been to freeze national security assessments on the day a license is granted.

Two years ago the United States Senate Committee on Homeland Security and Government Affairs Permanent Subcommittee on Investigations released a report on threats to United States networks from Chinese government-owned carriers. In it, they highlighted how the grant of authority to operate communications in the United States is typically a one-and-done activity. In other words, once an FCC license is granted, little is done to revisit the authority and safeguard our networks against evolving threats over time.

Here is why that matters. Under Section 214 of the Communications Act, the FCC is charged with granting applications for licenses to provide service in the United States. When we do this for carriers with foreign ownership, the agency relies on our national security colleagues to identify any issues that might need to be addressed. There is some back-and-forth in this process that can result in an agreement with the foreign carrier to mitigate any security risks identified at the time of the application. But once the FCC grants the authorization and agreement, that review is essentially frozen, even if national security considerations change.

In fact, there is currently nothing in our rules that requires the FCC or national security agencies to generally reassess a foreign carrier's authorization to provide service. This is in stark contrast to most other authorizations granted by the FCC that must be considered on a periodic basis. That is why the Subcommittee recommended requiring some review of Section 214 authorizations to account for evolving national security risks. I think that is a good idea. So stay tuned because I will soon share with my colleagues a rulemaking to explore this concept. I believe we can modernize our process to address these concerns while ensuring that the United States honors the expectations of Section 214 license holders so that the United States remains a safe and attractive place to do business.

The ten efforts I just outlined are full of details but they all serve one big idea—and that is making sure that the FCC uses every tool it has to address evolving threats to communications. The agency is doing more on this front than ever before. Because the opportunities and risks of next-generation networks are like nothing that has come before. So strengthening our policies at home is the right thing to do while we also increase our engagement with the world.

If we needed a further sign that this is the proper course, we have Doreen's historic election at the ITU. This recent vote is a reminder that the global community responds to our vision of communications. Because with our policies we seek to prove that security and democratic values do not merely co-exist; they build on and strengthen one other.

This event is testament to this, too. Because the work CSIS is doing to support United States leadership in 5G communications and security is important and so is the presence of both public and private sector interests here today. After all, working together is the only way to make progress. I am committed to that, and I know all of you are, too.

Thank you.