Remarks of FCC Commissioner Michael O'Rielly
Before the Daniel Morgan Graduate School of National Security
May 16, 2019

"China & International Telecommunications Union Issues Facing the United States"

I am incredibly honored to be here this afternoon. My deep thanks to Tom Cynkin for inviting me to join you. From the outset, it is a bit overwhelming to be among faculty and students with such great mastery of the doctrines, statutes, legal precedents, and current nuances related to national security law and policy. Anyone who has been immersed in national security matters knows that term is a bit amorphous and fraught with varied and even contrasting viewpoints. One man's favorite vacation picture in an airport or train station might be another's national security crisis. Fortunately, I am not here to discuss the scope or intricacies of the larger subject. After all, my expertise, to the extent it exists, is centered on national security within the much narrower context of communications policy.

My intention today is to outline the most recent actions of the Federal Communications Commission pertaining to the protection of U.S. national security, identify the difficult position in which we find ourselves with regard to Chinese telecommunications providers and manufacturers, and raise certain concerns with respect to the operations of the International Telecommunication Union, or the ITU as it is more commonly known. Hopefully, I won't disappoint, and will still have time to answer your questions.

To help frame the discussion, it seems appropriate to touch on why we expend so much energy protecting our national security. Of course, we do so foremost to prevent immediate threats and attacks on our homeland. And, our efforts can certainly reinforce unity and civic pride. Yet preservation of national security involves so much more. I see it as a mechanism and tool to ensure that America's preeminent value—individual freedom—is not jeopardized or surrendered at the hands of some other nation state or rogue group. Founding father John Adams wrote to his beloved wife, "Posterity! You will never know how much it cost my generation to preserve your freedom. I hope you will make good use of it." That ominous reminder reaffirms the underlying reasons for investing so much time, money, effort, and precious American lives to protect our national security. America serves as a unique experiment in the history of the world and freedom is at the epicenter of that creative effort.

Recent Commission Action

Within the universe of our existing authority, the Commission has been taking necessary and appropriate steps to protect and preserve our national security. While the Commission's jurisdiction in the national security area is not extensive, we have certain oversight abilities when it comes to those entities and services that we regulate. Specifically, the Commission has rules governing the review of media and telecommunications license applicants that exceed certain levels of foreign ownership, and the Communications Act prohibits foreign governments from holding an FCC license altogether.

When a company with a reportable level of foreign ownership files an application, the Commission also refers it to a group of Executive Branch agencies, commonly referred to as "Team Telecom." This group provides advice to the Commission on national security, law enforcement, and trade and foreign policy concerns that are outside the Commission's traditional expertise. With the advice of Team Telecom, the Commission has reviewed numerous applications involving foreign ownership. Those applications have either been approved on their face or pursuant to Team Telecom-led mitigation agreements. While this

system has generally worked efficiently over the last two decades, Team Telecom's process could certainly use some improvements, including a more formalized and streamlined structure and a firm timeline for making decisions.

Just last week, and for the first time ever, the Commission denied an application over national security concerns. China Mobile International (USA) Inc. requested in 2011—yes, over eight years ago—to provide international Section 214 services. For those of you who are not masters of Commission speak, that means the requisite approval companies must obtain from the FCC to transport communications between the U.S. and foreign destinations.

I think it is safe to say that, from the outset, the China Mobile application raised red flags with both the FCC and Team Telecom. By way of background, China Mobile USA, a Delaware corporation, is wholly owned by China Mobile Limited, a Hong Kong company, which is in turn owned and controlled by the Chinese government. The Commission ultimately found that China Mobile is "vulnerable to exploitation, influence, and control" by the Chinese government, and granting the license would jeopardize our national security and individual freedoms. In other words, providing China Mobile with greater access to U.S. telecommunications networks would have potentially given China—with its track record of computer intrusions, economic espionage, and other ongoing intelligence activities—access to information carried over our networks and the means to disrupt our communications.

In addition, Chairman Pai recently announced that the Commission is reviewing similar international 214 authorizations approved over a decade ago for other Chinese companies, including China Telecom and China Unicom. While China Mobile posed only a potential threat, these other companies have already had extensive access to our networks, and we need to know the extent of harm, if any, caused by this exposure.

Communist China

The FCC's concerns with respect to China extend well-beyond the licensing context. China, unlike most other countries, is attempting to monopolize the development and deployment of 5G technology and appears interested in using 5G network access for a variety of nefarious purposes.

It is important to note, at the outset, that the communist Chinese government and its "companies" are virtually one and the same. Not only is company leadership coterminous with Communist Party membership, but there is no refusing any government "advice" about operations or "requests" to assist the Chinese government's surveillance efforts. The government can also subsidize its providers, including through low-cost loans and unlimited operating capital, and thus allow wireless providers to offer competitive services below cost. This permits wireless providers to gain market share not only within China but internationally.

Many of these advantages also accrue to Chinese manufacturers. By providing below-cost equipment, throwing cheap labor at service projects, and engaging in intellectual property theft, Chinese manufacturers have been able to win contracts throughout the world. The ability to gain market share internationally is exacerbated by the export of Chinese equipment that is not compatible with other equipment brands, meaning that once a wireless provider or country invests in this equipment they are beholden to that Chinese manufacturer. This practice is more common than you may think.

Additionally, Chinese attempts to use international multi-stakeholder organizations to favor their manufacturers' technologies over others' continues to be extremely problematic. Standard-setting bodies establish the basic protocols and procedures to govern how networks operate, including technical specifications and interoperability guidelines. Yet we know that Chinese officials have tried to influence leadership positions within such bodies and block Western companies' technologies. This just amounts to another unacceptable mechanism to facilitate their global position in 5G.

Combined, these practices are resulting in the pervasive presence of Chinese equipment and providers in several nations' communications infrastructure, placing their national security at risk. As Chinese equipment and providers become ingrained in a nation's communications marketplace, the issues raised in the China Mobile order become evident: the Chinese government has the potential to access information that touches that equipment or is carried on that network. In our modern society, data and Internet networks are the core infrastructure for determining economic, diplomatic, and military might, and therefore constitute the battlefields that will define our future. We have an obligation to address this situation strategically and aggressively. Make no mistake, the U.S. will need to take every necessary precaution to prevent the current state of affairs from turning into an even more heightened, full-fledged international conflict.

The International Telecommunication Union

A few of you may be unfamiliar with the ITU, a largely unknown component of the United Nations whose primary mission is to harmonize global radio spectrum. Specifically, the ITU is the international body that convenes the World Radiocommunication Conference (WRC) where 190 or so countries meet every four years to negotiate and form consensus on how best to divvy up wireless frequencies for various uses—both new and old applications. In the intervening period between conferences, the ITU prepares studies in preparation for future meetings and operates as one of the standards-setting bodies for certain wireless functionalities. Knowing this, you may agree that its significance far exceeds its notoriety.

To give some context, global spectrum harmonization is the offering of commercial services on the same or nearby frequencies around the world. Doing so allows consumers to use the same devices at home and abroad and creates economies of scale by enabling research, development, and manufacturing costs to be widely dispersed, promoting investment and innovation while reducing the cost of devices and services for Americans. Thus, the more markets around the globe that use the same spectrum frequencies for the same commercial services, the cheaper and easier it is to get products throughout the entire ecosystem.

Given the recognized benefits of harmonization, what exactly is the problem with the ITU? The answer is multifold. First and foremost, it shouldn't be surprising that a multilateral subsidiary of the U.N. doesn't want to stay focused on its core mission. There is exceeding desire by many member states for the ITU to venture beyond its mandate and regulate the exciting new technology developments of the day, such as the inner workings of the Internet, artificial intelligence, cybersecurity, drones, and the like. In other words, the ITU wants to be the global regulator for shiny new things. While these matters are important, they generally aren't within the jurisdiction of the international authorities who attended ITU gatherings but are regulated by national—not international—regulators and agencies.

Second, the ITU has a problem whereby member countries try to ensure that "their people" staff the agency, even if to the detriment of the organization. These individuals operate with barely any

oversight or control by the elected ITU leadership, giving them free rein to pick and choose projects to pursue, hire favored and even biased technical consultants, set up questionable fora within which they can tilt the substance and skew the procedures to gain a desired result, and so on. In some regards, staff agendas—not member states—are driving ITU functions.

Third, elected leadership positions at the ITU tend to go to the next person in line, instead of the most qualified person or someone with a fresh vision, who is willing to reform its operations, or more importantly, follow its actual mission. As you can imagine, this tends to prolong stale thinking and allow management flaws to persist. The lack of a merit-based system for advancement and instead a reliance on longevity and entrenchment creates an environment inclined toward status quo and rent seeking by well-connected interests rather than cutting edge innovation and forward progress.

But, what does all this have to do with *our* national security? Let me explain. These structural and operational problems perpetuate a larger, more fundamental failing: the outcomes and debate surrounding recent spectrum policy decisions have come at the expense of U.S. interests and positions. In other words, the organizational body is frequently ruling against our views and requests, and that has an impact on our national security on multiple fronts. Those implications range from the rather benign—e.g., our perceived standing in the international community—to the serious—e.g., the health of our wireless providers, adoption of anti-U.S. industrial policies, and the long-term economic well-being of our nation.

The willingness of some countries to surrender their sovereignty to the whims of the so-called global community, or, more specifically, to those with ideologies opposed to our own, places U.S. interests at risk, as well as those of other like-minded countries. Should the WRC in November produce further unacceptable outcomes for the U.S., our need to re-evaluate our relationship with this body will become all the more apparent. As the largest contributor to the ITU's financing, the U.S. should expect a more balanced scoresheet when it comes to the agency's spectrum decisions.

Separately, it must be stated that the current secretary-general is a Chinese national and that obtaining the ITU head position was an important achievement for China. It has not gone unnoticed that this leadership role has been used both subtly and overtly as part of China's larger global play. Consider that the ITU signed a 2017 Memorandum of Understanding to expand worldwide technology infrastructure and Internet connectivity through China's own "Belt and Road Initiative." We cannot ignore the relationship between some current ITU policies and the grander goals to enhance mainland China. And, most importantly, we cannot dismiss the impact of such activities on the current and future national security of the U.S.

Executive Order on Supply Chain

Turning topics ever so slightly, I want to briefly discuss the recent Executive Order pertaining to protecting the communications and technology supply chain signed by President Trump yesterday afternoon. Under the text, the President directed the Secretary of Commerce, in consultation with the heads of other Executive agencies, to prohibit any transaction or use of communications technology or services supplied by entities owned, controlled, or subject to the jurisdiction of foreign adversaries. To be clear, this Order does not designate any specific countries or companies as risks, instead opting to place such decisions in the hands of the Executive Agencies to determine whether a transaction can raise national security issues. If there are national security implications, the Executive agencies have the ability to negotiate mitigation measures, if possible, or prohibit the technology or services altogether.

I appreciate the President's recognition of the importance of this nation's communications infrastructure and this strong effort to protect against U.S. adversaries who may be "creating and exploiting vulnerabilities" to engage in "malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people." This aggressive and decisive action will serve as a forceful tool to help minimize this national security threat.

* * *

I'll stop there, so that we can turn to the inquisition – I mean, discussion portion – of today's event. Trust me, I hope to learn as much from you about the national security landscape as I hope you will learn from me about the global telecommunications marketplace and corresponding security concerns.