KEYNOTE SPEECH OF COMMISSIONER NATHAN SIMINGTON TO NOVEMBER 2021 APCO EMERGING TECHNOLOGY FORUM

Good evening. Thank you for asking me to speak to you today. APCO members do some of the most important work in the country, and supporting you is a priority for me and my colleagues at the FCC.

The public relies on you to get them help when they need it most, and first responders rely on you to keep them informed and connected when every second counts. So the reliability and security of your networks is of the utmost importance. The FCC is doing a lot of work to ensure that your needs are met—from improvements in network outage reporting, to smarter approaches to foreign security threats to American networks, to the transition to next-gen public safety networks.

With the wide adoption of 5G around the corner, getting these issues right is more important than ever. Decisions made in the near future—by the communications industry, by public safety bodies, and by government and regulators—will determine what the public safety communications landscape looks like for years to come. So today I plan to touch on what I think are some of the most important public safety communications issues, as well as what I think the FCC and industry can do to make sure that the transition to the next generation of public safety communications infrastructure is a success for the people who use it and the people that they serve.

For twenty years now, high hopes for public safety use of the 4.9 GHz band have been unrealized, and this increasingly valuable spectrum has mostly lain fallow. This situation does not serve the public safety community well, but the solution is to find uses for the band that do. I'm happy that my colleagues at the FCC have agreed to explore an exclusive-use licensing model for commercial use of this band. I think an exclusive-use licensing model will prove more beneficial—operationally and economically—than the either the current model or any of the other alternatives explored by the FCC in recent years. An auction of exclusive use licenses for 5G and other advanced services would harvest the most value for the 4.9 GHz band, as we saw with the C-Band auction. And it will lead to a more robust 5G equipment ecosystem that public safety licensees operating in the band need to accomplish their important work.

The incentive auction approach, which could provide enormous value to those who choose to relocate from the band, will provide current licensees with the funds to pursue whatever technology strategy they decide best suits their needs, whether it be deploying or expanding traditional LMR systems, investing in modern alternatives provided by commercial vendors, or using the funds for something else altogether. And it accomplishes all this while still allowing those who have chosen to develop their own 4.9 GHz infrastructure to keep their license should they wish to. This way, current licensees will be able to decide for themselves which tech strategy will work best for them without relinquishing any equipment or access

unless it's their choice to do so. It will work better both for those who wish to continue use of 4.9 GHz and those who would prefer to be made whole and then use other bands.

As for development of the 4.9 GHz band itself, an exclusive-use licensing model is best for mission critical services. In order for an ecosystem of fit-for-purpose equipment and vendors to emerge, we need large-scale commercial investment in these bands. And basing public safety infrastructure on cutting edge commercial technology will mean a stronger market for the necessary products and services, so that public safety bodies can pay competitive prices for top-of-the-line equipment instead of exorbitant sums for bespoke and inferior special purpose gear based on commercially abandoned technologies.

Seeking comment on these proposals will make sure that we get this important decision right. We are not omniscient at the FCC. I have never run a PSAP—or any public safety infrastructure for that matter—but you have. I look forward to hearing what you have to say. We can't get this right without you.

The FCC also has an important role to play in helping you stay safe from attacks on your communications systems. The FCC has exclusive authority over non-federal spectrum allocation and end user device certification. That puts us in a unique position to ensure that those devices are secure. Now, I am not suggesting that the FCC should drive outside of its lane. We aren't a cybersecurity agency. It would be wasteful, redundant, and, frankly outside of the FCC's practical capabilities to take the lead on the development of general cybersecurity standards. That job will need to fall on other parts of the federal government who do have that capacity, such as the Department of Homeland Security.

However, it is in everyone's interest to have a rapid uptake of secure, reliable, low-latency, high-bandwidth wireless technologies integrated into all aspects of daily life—the 5G transition. And to succeed, such integration will require public buy-in. No one will support it unless it offers reliability and security superior to that provided by current technologies. But beyond the average commercial user, public safety users have, of course, much higher reliability requirements than we see in general commercial products, and it is absurd for the federal government to expect buy-in from public safety in particular until 5G security, in all aspects, is beyond question.

Many current technologies are basically consumer-grade or, if they're industrial, nevertheless increasingly unfit for purpose. Attacks are getting easier, and our systems have not kept pace. Countless schools, governments, and companies have been paralyzed by low-effort ransomware attacks; serious infiltrations of US government systems have damaged the security of the country; low-cost attacks have undermined the security supposedly offered by smart cards and smart locks; and the theft of private information has become routine. Frankly, while there are bright spots here and there, overall, the current digital ecosystem is built on insecure foundations. In the early days of microcomputers, no one was thinking very hard about security, and we owe

the advanced capabilities we rely on daily to that technical revolution. But I can't help but think that, if security had been a consideration since day 1, we would have built completely differently. It's time for the FCC to do its part in clearing this technical debt.

Much more should be required of the minimum viable product for high-security, high-reliability applications such as those contemplated under the 5G transition and required for its success. This is where the FCC has the unique ability to act, by encouraging industry and government bodies to adopt security standards for at-risk consumer grade devices that require FCC approval. These standards can then be integrated into the FCC's equipment authorization rules. While it is possible that these standards may moderately increase the cost to manufacture certain devices, we cannot risk billions of dollars of damages down the line--to say nothing of human lives--just to save a buck upfront.

One specific threat, much on everyone's minds, is foreign powers taking control of our communications infrastructure. The ability of federal, state, and local governments to respond to disasters, natural or manmade, cannot depend on the benevolence of the Chinese government. Nor can sensitive information about public safety capabilities and shortfalls—information inherently gathered by the operation of those systems—be handed over to our rivals on a silicon platter.

I've been honored to support Commissioner Carr's great work in this area, and I'm also encouraged by Congressional initiatives like the bipartisan Secure Equipment Act, recently passed in the House and awaiting passage in the Senate, which will further protect our networks from the risk of foreign control. In the future, we need to look not just at where equipment was built, but also at how trustworthy it is in operation. It would be self-defeating to ban untrustworthy equipment from our networks, only to put the ongoing operation of these networks in the hands of untrustworthy actors anyway.

A related issue is the resiliency of the networks and equipment used to deploy the next generation of public safety communication and infrastructure systems. Let me begin with an analogy to the current crisis.

During this pandemic, the fragility of the global supply chain has been exposed. The shutdown of a small country half-way around the world can quickly translate to shortages of goods on shelves across America. And whereas in the past, larger inventories would give manufacturers and suppliers time to adapt to changing circumstances before average consumers ever experienced shortages, the aggressive efficiencies and lean inventories of modern businesses have ironically made us more likely to see empty shelves in times of crisis.

Similarly, complex digital systems are vulnerable to single points of failure, feedback loops, cascading failures, and other phenomena that contribute to overall fragility in the face of the unexpected. And just like with manufacturing supply chains, aggressive efficiency and cost-cutting can go too far and create fragile systems that lack redundancy and the capacity for

unexpected load. I would imagine that the public safety community has painful stories about capacities that are costly to acquire and are rarely needed -- but when they're needed, they're needed desperately.

The periodic failure of equipment and systems should be treated as inevitable, not impossible, and it cannot be that such failures—most likely to happen at the worst possible times, when the demands on the systems are highest—leave the public without access to police during crises or firefighters during natural and manmade disasters. These failures lead to the unnecessary loss of life, but also long-term damage to public trust, and the transition to advanced public safety systems must leave us better off, not worse. Like with cybersecurity, the FCC's licensing power will be an important tool in ensuring that the public safety systems of the future are resistant to such failures.

On the topic of resiliency, I strongly support the NPRM adopted by the Commission in late September. It takes a close look at how the FCC's current disaster procedures, such as DIRS, can be improved. And specifically, I think it's a very good idea to see how the FCC, service providers, and power companies can coordinate more effectively during disasters.

When we go back to having a five-member commission, the return of Title II regulation of internet service is a real possibility. That could include restrictions or bans on internet fast lanes, zero-rating, and other such traffic management techniques. I'm not here to talk about the pros and cons of Title II regulation overall, but whatever happens, the commission must make sure that any regulation that we do impose does not harm the ability of police, firefighters, and other public safety bodies to communicate and coordinate in the midst of an emergency.

Whatever the commission decides to do about broadband fast lanes, we should be careful to allow the prioritization of public safety traffic. Carriers should not be punished if they make Netflix streams take a back seat to real time video from firefighters in dangerous, high-stakes conditions. Similarly, carriers should be allowed to offer plans that zero-rate—that is, that don't count against monthly data caps—for communicating public safety data among government bodies and with the public.

Before finishing, I want to briefly touch on two more things.

First, 911 services. The FCC's work here is vital: mitigating 911 fee diversion, improving 911 reliability through improved communications between network operators and PSAPs, and of course, the desperately needed Z-Axis implementation. On this last point, I want the carriers to move as quickly as they can to provide this crucial location information to first responders, and I'm sure that many of you feel the same. Further delay is unacceptable, and I'm hopeful that the accommodation reached on Z-Axis will be the first and the last.

Second, emergency alerting. ATSC 3.0 broadcast technology has the potential to genuinely change the way that the public receives emergency alerting, and it's something that I

am really excited about. Broadcasters can use the new IP-based broadcast standard to send alerts to precisely defined geofences and to send supplement the alerts with rich and interactive information, including, for instance, the path of a tornado and likely times that individual households may be affected. The more specific our disaster information is, the more effective our responses can be, allowing public safety to go straight to the danger and preventing needless responses. I'm eager to see this technology deployed and for you to be able to better serve the public with it.

At the commission, we take our duty on public safety matters seriously. Your work quite literally saves lives. My staff and I are committed to working with you to make America's public safety infrastructure as strong as it can be, and our door is always open to your suggestions and feedback. Again, thank you for the invitation, and thank you for listening to my remarks. I hope your conference is a success.