Attachment—Additional Questions for the Record

Subcommittee on Communications and Technology
Hearing on
"Accountability and Oversight of the Federal Communications Commission"
December 5, 2019

The Honorable Jessica Rosenworcel, Commissioner, Federal Communications Commission

The Honorable Anna G. Eshoo (D-CA)

1. **The decision to increase minimum service standards was proposed in conjunction with a port freeze. Coupling these items was essential for increasing service, while also reducing waste, fraud, and abuse. Why is the FCC moving forward with just increasing minimum service standards which has caused carriers to cease providing Lifeline services?**

Response: In 2016, the Federal Communications Commission decided to modernize the Lifeline program for the broadband era. As part of this effort, the agency committed to a series of changes that over time would reduce support for traditional telephony and increase the focus of the program on broadband. The agency also set up a 12-month port freeze for Lifeline-supported broadband service in order to "incentivize greater up-front investments from providers" in "broadband-capable devices and services."

However, in the intervening years it has become apparent that those who rely on Lifeline still depend deeply on the program for voice services. In other words, while the market has evolved, it has not moved precisely in the way we imagined it would when these policies were put in place in 2016.

As a result, a coalition of carriers and Lifeline advocates petitioned the FCC to pause the changes to program support that were slated to take place in 2019. I believe they made a compelling case that additional study was warranted before allowing further adjustments to the program's minimum service standards. In fact, I think the agency should have pursued such study in order to better understand current and future needs of Lifeline program recipients. However, in a decision in November 2019, the FCC chose a different course. Instead of pausing for further study, the agency adjusted the minimum service standards for data for Lifeline offerings for the following year.

I am concerned that the agency's action did not do enough to provide this program with the certainty it needs. That's because without pausing for review at this time, the FCC will be back in the same place, wrestling with the same issues, and dealing with another set of scheduled service adjustments to our minimum standards at the end of this year.

2. **The FCC found that "the large increase in the minimum standard for mobile broadband usage could unduly disrupt service to existing Lifeline subscribers." Would the FCC suspend the implementation of next year's minimum service standard if a similarly large increase is anticipated again?**

Response: Unfortunately, over my dissent, the FCC's November 2019 decision regarding Lifeline minimum service standards did not provide the program with the certainty it needs. As a result, it seems likely that the FCC will have to revisit its Lifeline minimum service standards again later this year. When it does, I hope that the agency will conduct a more thoughtful assessment of the program in a manner that helps ensure its stability.

3. **Is the FCC considering opening a new proceeding to revisit the appropriate formula for calculating minimum service standards for Lifeline mobile broadband service?**

Response: In the period following the 2016 decision modernizing the Lifeline program, it has become apparent that those who rely on Lifeline still depend deeply on the program for voice services and the formula put in place to update data minimums may have unintended consequences. In other words, while the market has evolved, it has not moved precisely in the way we imagined it would when these policies were established in 2016.

Recognizing that our rules are not working as intended, I did not support the FCC's decision in November 2019 to only adjust minimum service standards for broadband services for a 12-month period. I believe that a better course of action would have been to pause further adjustments of the minimum service standards pending completion of the FCC staff's State of the Lifeline Marketplace Report due on June 30, 2021. This would permit the agency to assess what changes, if any, are necessary, informed by actual data about the marketplace. Though the agency did not choose to proceed this way, it could still examine what measures are needed to bring stability to the Lifeline program, including a thoughtful assessment of the operation of its minimum service standard formula.

4. **You've raised network security issues as a major concern of yours. Beyond supply chain issues, which the FCC and our Subcommittee have worked on, what other recommendations can you make relative to securing our nation's wireless networks—for example, addressing SIM swaps, carriers' usage of dated encryption and authentication algorithms, and the threats of cell simulators or IMSI catchers?**

Response: The very first sentence of the Communications Act tasks the agency with a duty to "make available, so far as possible, to all the people of the United States . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service for the purpose of the national defense" and for "promoting safety of life and property." Accordingly, the FCC has a clear mandate to help ensure the safety and resiliency of our nation's communications networks.

To this end, the agency needs to address communications vulnerabilities like SS7. SS7 is a signaling protocol that permits carriers to communicate with one another to deliver calls and text

messages between and among their networks. While SS7 offers practical benefits, it is known to have significant cybersecurity problems. It is well understood that criminals and foreign governments can exploit flaws in SS7 to track mobile users, intercept calls and texts, and even steal sensitive information available on devices.

The FCC is uniquely situated to comprehensively address problems with SS7—and has both the network expertise and statutory authority to do so. To date, the FCC's Communications Security, Reliability, and Interoperability Council recommended that communications service providers implement specific security measures to help prevent exploitation of the SS7 network infrastructure. The FCC's Public Safety and Homeland Security Bureau, in turn, released a Public Notice recommending that communications service providers implement these measures. The Bureau also sought comment on the progress being made to address SS7 vulnerabilities. At this point, The FCC needs to move beyond studies and voluntary recommendations to ensure that the measures identified by CSRIC are implemented in a timely fashion.

In addition, in 2018 press reports revealed that our networks may be vulnerable to surveillance by IMSI catchers, or stingray devices, including in Washington. These surveillance tools can transform cell phones into real-time tracking devices by mimicking legitimate cell towers and some may even have the capability to record the content of calls. Moreover, there is reason to think that use of these technologies may violate statutory prohibitions against causing harmful interference and requiring a license or authorization to transmit. The security of our communications is at stake and the FCC should do more than offer just silence in response to these reports. At a minimum, the agency needs to explain how foreign actors may be transmitting over our airwaves without approval from the FCC.

The problem of SIM card swaps—in which hackers can steal your mobile identity—also needs attention from the FCC. At its most basic, a SIM swap occurs when someone convinces a mobile carrier to switch a phone number over to a SIM card they own. By diverting incoming messages, scammers can easily complete text-based two-factor identification checks that protect a victim's most sensitive accounts. Press reports have documented a number of incidents in which SIM hijackers drained thousands of dollars—and in one case, $23.8 million worth of cryptocurrencies—out of people's accounts. Other countries are taking steps to mitigate this problem, but so far the FCC has remained silent. I believe that it is important that the FCC seek to understand this growing threat, take steps to encourage carriers to discontinue using insecure methods of customer authentication, and explore the authority it has regarding customer proprietary network information to more broadly protect consumers.

Finally, the FCC must recognize that the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks. That means we also need to focus on the security of the connected things, otherwise known as the Internet of Things. To do so, the agency can begin by taking a fresh look at its existing practices. Right now, every device that emits radiofrequency at some point passes through the FCC. This routine process for equipment authorization takes place behind the scenes. But we could have the FCC use this process to encourage device manufacturers to build security into new products. In addition, we could work with the National Institute of Standards and Technology to do it. That's because just last year, 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. Once the NIST process is finished, we could take that work and update the equipment authorization process at the FCC. In doing so, we could turn the Internet of Things into the Internet of Secure Things.

5. **Some are proposing allocating spectrum in the 6 GHz band for licensed use, by relocating incumbents to the 7 GHz band, though that band is currently occupied by government entities, including the Department of Defense. How long has the FCC been working with the federal government on allocation of 7 GHz?**

Response: As you note, the FCC currently is reviewing proposals compiled in our ongoing proceeding involving the 6 GHz band, including proposals to relocate incumbents to the 7 GHz band. My office is not aware of any substantive discussions with other federal agencies regarding this proposal. However, such discussions are likely to take place first and foremost with the office of the Chairman.

6. **As you have recognized, the need for unlicensed spectrum is as high as ever, and it's growing. Some have raised concerns about harmful interference to microwave services if unlicensed devices would be allowed to operate in the 6 GHz band. Do you have the data necessary to create rules for these two services to coexist?**

Response: Wi-Fi is a powerful force in the digital economy. It can provide a jolt to the Internet of Things and foster massive innovation without the challenge of requiring a spectrum license. We need more of it—and the 6 GHz band is the right place to start. The technical studies in the record at the FCC suggest that there could be opportunities to introduce unlicensed services in this band without causing harmful interference to vital, point-to-point microwave communications throughout the country. To this end, the FCC is exploring technology to further mitigate the risk of interference to incumbent services by prior coordination of unlicensed operations. In addition, the FCC has requested comment on a variety of additional mitigation techniques to protect these important services. My office is reviewing the substantial record before us and the technical data that has been collected in conjunction with this proceeding. I remain hopeful that we can make greater use of this valuable spectrum resource without harming existing uses.

7. **One promising innovation in wildfire mitigation is the Falling Line Conductor that uses low-latency, private LTE networks to depower a broken line before it hits the ground and becomes a fire hazard. Do you have a view on how such technologies can help mitigate wildfire threats and the need for preemptive electrical shutoffs? When will the FCC complete its 900 MHz proceeding that impacts the ability of utilities to use such technologies?**

Response: The timing of the 900 MHz proceeding rests with the Chairman of the FCC. The record that has been compiled in this proceeding highlights a variety of use cases for private LTE networks that could help utilities continue to deliver safe and reliable power to their customers. This includes Falling Line Conductor capability, which would use 900 MHz private LTE

broadband to de-energize a power line that has broken, before it can hit the ground and cause fire. Our record demonstrates that some utilities, particularly in California, are interested in this kind of low-band private LTE service and its ability to prevent fires.

In addition to completing the 900 MHz proceeding, the agency must do more to ensure the resiliency of our networks in the face of disaster. After all, public safety is an essential part of the FCC's mandate. But on too many occasions when disaster has struck, our communications have failed. This is happening with disturbing frequency in the aftermath of major weather events, including recent hurricanes and wildfires. In light of this, I believe it is time for the FCC to update its policies regarding network resiliency. First, the agency needs to address the reported deficiencies in its wireless network resiliency policy. Two years ago the Government Accountability Office criticized the FCC for its limited oversight of this framework, but in the interim time the agency has done no more than issue a series of public notices seeking comment on the problems. Second, the agency should update its policies regarding network outage reporting. When our networks go out, so much of modern life grinds to a halt. However, our outage reporting requirements are outdated, because they are generally limited to traditional telephony. In the broadband era, these policies need an update. Third, the FCC must standardize its reports of outages following a major weather event or disaster. Ideally, the agency would release an assessment within several weeks of a major incident. It is simply not acceptable, as was the case following Hurricane Maria, for the agency to wait a year before publishing such a review.

8. **On June 11, 2019 at a USTelecom Forum on robocalls, Chairman Pai said "Now that the FCC has given you the legal clarity to block unwanted robocalls more aggressively, it's time for voice service providers to implement call blocking by default as soon as possible." I couldn't agree more. Have carriers responded to this call to action? Have companies raised legal, technical or other objections with these actions requested?**

Response: Robocalls are getting worse and consumers are paying the price. For this reason, I was pleased to support, in part, the FCC's decision in June 2019 that allowed carriers to offer opt-out call blocking services to consumers. Since that time, some carriers have offered tools to help consumers block unwanted robocalls while others have indicated that they are evaluating their options. I believe the FCC should continue to monitor how these tools are deployed and how effective they are at screening out robocalls. To this end, in December 2019, the FCC's Consumer and Governmental Affairs Bureau issued a public notice seeking comment on the implementation of call blocking tools.

However, I believe there was one fundamental mistake in the FCC's June 2019 decision. Over my objection, the agency did not require that these call blocking tools be offered for free to consumers. This is not right. Consumers did not create this mess with robocalls so they shouldn't have to pay to fix it. The good news, however, is that the TRACED Act, which was recently signed into law, took a different approach. In this new statute, Congress required the FCC to go back and fix this problem and ensure call blocking is available free to consumers. Under the TRACED Act, the FCC also has a number of new duties relating to robocalls. It is

essential that the agency meet all milestones in this law and work to ensure it does so in a consumer-friendly and responsible fashion.

9. **At the same USTelecom event in June, Chairman Pai said that "USTelecom has been particularly helpful in making sure that we can quickly trace scam robocalls to their originating source." How successful has USTelecom's Industry Traceback Group (ITG) been in combatting robocalls?**

Response: As you note, there is an effort underway in the industry to identify the network source of robocalls. This work involves tracing just where robocalls are first introduced to our networks, in light of the fact that a single call may travel over multiple carriers. For instance, if there is a call from Augusta, Maine to Anaheim, California, it is unlikely that one carrier is responsible for the call from coast to coast. Instead, after one carrier initiates the call it will likely be handed off to a series of different carriers before it reaches its destination. This is a lot like taking a series of connecting flights on different airlines to travel across the country. Finding where illegal robocalls start in this system requires reverse engineering these handoffs in order to "traceback" where they were first put on the line. This is important because the carrier at the start of the call path may have a financial incentive to allow illegal robocalls to get on the line or may find it convenient to take the money and look the other way. Through this process, I am hopeful we can pinpoint the carriers that are the source of this problem and put them on notice that they are facilitating bogus calls.

The bulk of this effort has taken place through USTelecom, an industry trade organization. I think it's time for the FCC to get more involved. Right now, there is no public process for holding carriers who put this junk on the line accountable. There needs to be one. In addition, I think the agency should explore how carriers that repeatedly engage in this behavior may be subject to either enforcement penalties or even loss of authorization from the FCC.

10. **A *Wall Street Journal* article titled "Small Companies Play Big Role in Robocall Scourge, but Remedies Are Elusive" states that "The FCC has asserted limited jurisdiction over VoIP providers, an agency spokesman said." What prevents or limits the FCC from using existing statutory authority to take enforcement actions against VoIP providers?**

Response: Robocalls are a serious nuisance and their numbers are growing. At the start of this Administration, consumers received roughly 2 billion robocalls a month. They now average between 5 and 6 billion a month. What we have done to date to stem this tide is clearly not enough. So it's unacceptable for the FCC to throw up its hands and suggest it will not use the full extent of its authority to fix this problem. Moreover, to the extent that there are any gaps in its authority the agency should identify them and seek assistance from Congress to help address how they can be narrowed.

The good news is that in the TRACED Act, which was recently signed into law, the FCC is required to finally take action when it comes to VoIP providers. Specifically, the FCC is required to conduct a study regarding the feasibility of a registry of VoIP providers and consider requiring VoIP providers to retain call records in order to assist with call traceback.

11. The FCC's "Report on Robocalls" (CG Docket No. 17-59; February 2019) states that "Five providers that had been identified as uncooperative in traceback have taken steps to participate going forward." Have these five providers continued cooperating with traceback efforts? Do *any* providers remain that are not being cooperative?

Response: As you suggest, in the FCC's February 2019 Report on Robocalls, the agency acknowledged that after public letters were sent by senior FCC officials to certain companies, those companies then took steps to participate in the industry traceback effort.
The lesson here is important: The FCC should be doing more to shine a light on robocalls.

The Honorable Peter Welch (D-VT)

1. A lack of broadband connectivity can impact all aspects of our lives: keeping children on the wrong side of the homework gap from realizing their full potential, posing barriers to telehealth solutions that can improve care, keeping farmers from capitalizing on advancements in precision agriculture, and limiting economic opportunities for workers and small businesses. However, I have been encouraged by the Commission's support of innovative solutions, specifically TV white space, that can enhance the pace, reach and cost-effectiveness of broadband deployment in rural communities. The adoption of a final order in the TV white space (TVWS) reconsideration proceeding earlier this year marked an important first step, and I encourage the Commission to build on this step by issuing a Further Notice of Proposed Rulemaking (FNPRM) to address remaining regulatory hurdles to greater TVWS deployment as soon as possible. By taking this step, the Commission can update its rules surrounding TVWS, which will increase the potential for rural broadband deployment and, subsequently, the availability and adoption of Internet of Things (IoT) applications throughout rural areas.

a. Will the Commission make the adoption of a TV White Space Further Notice of Proposed Rulemaking a priority to complete as soon as possible and no later than the first quarter in 2020?

Response: While white spaces innovation began here in the United States, in recent years the use of this technology to bridge digital divides has advanced faster in other nations. At present, there are more than 20 television white spaces projects worldwide that are serving more than 185,000 users. However, in the United States, deployment of this technology has stalled, in part due to outstanding regulatory issues.

Decisions regarding when and how these issues are addressed lie with the Chairman of the FCC. Last year the FCC adopted an order that took steps to improve the accuracy and reliability of white spaces databases. But I believe that much more work needs to be done to address remaining regulatory barriers. To this end, I believe the FCC should resolve outstanding

petitions for reconsideration involving white spaces activity. In addition, the agency should explore additional rule changes to facilitate connectivity. I would fully support a further notice of proposed rulemaking to do so, just as you recommend.

The Honorable Tom O'Halleran (D-AZ)

1. **Commissioner Rosenworcel, as rural communities begin gaining more access to modern broadband technology, I believe it is imperative that communities are empowered to understand how to best use broadband to thrive with e-learning, access telemedicine, and compete in our global economy. I also understand schools, libraries, and community centers in rural areas have begun local digital literacy training programs to teach communities how to leverage modern applications through the internet.**

    a. **How can the FCC incentivize the creation of more digital literacy training programs for rural communities?**

Response: Digital literacy is a significant challenge in the United States. While technology may feel ubiquitous in many communities, there are populations across the country that are still outside its everyday reach. To this end, data from the Pew Research Center found that a majority of adults in this country can answer fewer than half the questions correctly on its digital knowledge quiz and many struggle with basic cybersecurity and privacy questions.

It's apparent that we need to do more to extend digital age opportunity to all. In 2017, the FCC created a brand-new organization within the agency: The Office of Economics and Analytics. Since its creation this office has published just two white papers—one involving broadband access in multi-tenant environments and another about the organization of economists in regulatory agencies. I think that the Office of Economics and Analytics should be charged with surveying digital literacy efforts across the country in order to create a national repository for information on digital literacy and developing a set of targeted best practices.

    b. **What role can discount internet offerings from internet service providers to persons already in federal assistance programs (food stamps, housing, etc.) further increase broadband *adoption* in rural communities? Has the FCC examined adoption rates in light of these programs?**

Response: FCC data show that more than one-third of households nationwide do not subscribe to broadband. In rural and Tribal areas, the adoption challenge is even more profound.

Both private and public efforts are needed to help address this national challenge. To this end, some internet service providers offer discounted offerings for qualifying low-income Americans. These industry efforts would benefit from further promotion and expansion. Meanwhile, the FCC is responsible for the Lifeline program, which provides a monthly discount on service for eligible low-income subscribers. This program is limited to one subsidy per household. There are a variety of ways for an individual to qualify for the program, including having an income

135% or less than the federal poverty guidelines. In addition, individuals can qualify by participating in a variety of federal assistance programs, including the Supplemental Nutrition Assistance Program (SNAP), Medicaid, Supplemental Security Income, Federal Public Housing Assistance, Veterans Pension and Survivors Benefit, as well as certain Tribal programs. Going forward, however, it is essential that the FCC continues to work to improve the National Verifier—the online portal used to qualify applicants for the Lifeline program. At present not all of these assistance programs are in the verifier system, causing difficulties for applicants. The FCC needs to fix these problems as soon as possible.

c. How can schools and libraries continue to play a critical role in expanding Wi-Fi hotspot lending programs to students to help close the homework gap?

Response: This is a terrific idea. Today, seven in ten teachers assign homework that requires internet access. But data at the FCC suggest that roughly one in three households do not subscribe to broadband service. Where these numbers overlap is the homework gap. The Senate Joint Economic Committee has studied this problem and determined that it affects as many as 12 million students nationwide.

You see them in communities across the country—lingering in the library, hanging out in school parking lots, or sliding into booths at fast food restaurants—going wherever they can to get the online signal they need to complete nightly schoolwork.

We should do better by these students. There are programs today in libraries from Maine to Missouri that loan out wireless hotspots. These are invaluable for anyone in a household without reliable and consistent access to the internet. They are especially critical for students who do not have the broadband at home they need to do their homework. Accordingly, it's time to ask how we can expand such programs and what role Congress and the FCC can play to help make that happen.

Working with Congress, the FCC could establish a national fund to solve the homework gap and do so by using a portion of the funds raised from the future sale of spectrum. In other words, the homework gap is a public problem, so let's use resources from public airwaves to fix it. This could be done, for instance, with the 3.7-4.2 GHz band or with any other airwaves that may be the subject of upcoming legislation. The fund established could help, for instance, support the availability of wireless hotspots in every school library across the country. It could also help make more school buses wi-fi enabled. This would turn ride time into connected time for homework and would be especially valuable in rural areas where so many students spend hours on a bus simply to get to and from school every day. If we did this, we could help ensure that every student has a fair shot at success in the digital age and that no child is left offline.

The Honorable Greg Walden (R-OR)

1. **As I stated at the hearing, ending diversion of 9-1-1 fees is a priority for me. According to recent reports submitted to Congress pursuant to the New and Emergency Technologies 9-1-1 Improvement Act of 2008, states and taxing jurisdictions are still diverting 9-1-1 fees for purposes other than 9-1-1. What statutory tools would be useful for the Commission, or other entities, to stop states from diverting 9-1-1 fees?**

Response: 911 fee diversion is a form of fraud. It needs to stop. To this end and pursuant to the NET 911 Improvement Act, the FCC publishes a report on the state collection and distribution of 911 and enhanced 911 fees and charges each year. This is an important report because it shines a light on the states and localities that engage in 911 fee diversion. Nonetheless, some fee diversion continues. So it may be time for Congress to revisit this law and identify what other things we can do to prevent diversion going forward.

In the past, I have worked to draw attention to this issue with my colleague Commissioner O'Rielly. Together we have explored some ideas to disincentivize diversion, including prohibiting representatives from states that repeatedly divert 911 fees from participation on FCC advisory committees and prohibiting fee-diverting states and localities from any federal support dedicated for 911 system upgrades in any new infrastructure legislation.

The Honorable Robert E. Latta (R-OH)

1. **As the author of the Precision Agriculture Connectivity Act that was included in last year's Farm Bill, I am interested in the economic benefit of GPS to the agriculture sector. Talking to farmers in my district, I know GPS can improve farm planning, field mapping, soil sampling, tractor guidance, crop scouting, variable rate applications, and yield mapping. All this innovation relies on connectivity, including that provided by GPS. How will the Commission continue to protect GPS services from harmful interference?**

Response: A few months ago, I visited Pape Farm in Dyersville, Iowa and saw firsthand how precision agriculture can improve farm planning, field mapping, soil sampling, tractor guidance, crop scouting, yield mapping, and more. I recognize that Global Positioning Signals are fundamental to all of this activity. Moreover, outside the farm, we count on GPS to navigate our roadways, track our misplaced devices, check in on social media, and support bank transactions, shipping systems, and our national power grid. In addition, our military depends on GPS for everything from search-and-rescue missions to missile strikes.

For all of these reasons, GPS is an important part of our national and economic security. That's why a little over a year ago, the FCC augmented our GPS system by permitting consumers and businesses in the United States to supplement GPS with the European global navigation satellite system, known as Galileo. Going forward I believe the FCC will need to continue to review

GPS use to ensure that it remains safe from harmful interference and that it can continue to support economic innovation in agriculture and so much more.

The Honorable Adam Kinzinger (R-IL)

1. **During the hearing, I asked Chairman Pai the following questions:**

   Are there cybersecurity or physical security concerns if information and communications technology companies allow non-cleared or un-vetted personnel access to software development kits or application programing interfaces for 5G networks?

   Is there a common standard to use vetted personnel, AI, or machine learning to analyze source code that will be distributed or used in patches for software updates of 5G equipment?

   While the Chairman provided thoughtful answers in response, I ask that the Commission follow up with the Committee to offer any supplemental information or ideas regarding the ways in which the Commission, using existing authorities, or Congress, by enacting new legislation, can bolster the physical security and cybersecurity of our 5G networks. Please be as detailed as reasonably possible, and if the Commission feels that these responses are best conveyed to the Committee in a confidential manner in order to protect our national security, please indicate as much to the Committee and we will work with you all to make appropriate arrangements.

Response: 5G requires new approaches to security across the board—including physical security. Unlike prior generations of wireless technology, 5G small cells will add a whole new and denser layer of equipment to our world. Networking equipment, storage, computing hardware, and other valuable infrastructure will be located much closer and be more accessible to the public—in cities and housing developments, commercial and industrial locations, and along roads and highways. These facilities also will be accessed routinely by employees, technicians, and contractors, often times from several different companies or subcontractors.

On top of that, 5G networks will move away from centralized, hardware-based architectures to distributed, software-defined networking. While this offers many compelling benefits, it also could create security risks.

Securing widely dispersed and software-based 5G systems is crucial. The Department of Homeland Security's Information and Communications Technology Supply Chain Risk Management Task Force currently is identifying and evaluating threats to ICT supplies, products, and services and producing policy recommendations. Right now, the Task Force is finalizing its work streams for its second year. Its membership and scope make it an ideal place to advance discussions about physical security of 5G networks. In addition, the National Telecommunications and Information Administration has launched a multi-stakeholder process

on software component transparency, with the goal of increasing transparency around the use of software components so that when vulnerabilities are detected, there is a way to quickly remedy problems. The FCC should work with these agencies and others to better understand companies' practices in terms of restricting access to software development kits or programming interfaces for 5G networks to vetted personnel; developing common standards for software patches of 5G equipment; and ensuring physical security of 5G infrastructure.