Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting the Deployment of 5G Open Radio Access Networks	)	GN Docket No. 21-63
	)	

COMMENTS OF AT&T

AT&T SERVICES, INC.
208 S. Akard Street
Rm 3011
Dallas, Texas 75202

Robert Vitanza
David J. Chorzempa
David L. Lawson

April 28, 2021

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting the Deployment of 5G Open Radio Access Networks	)	GN Docket No. 21-63
	)	

COMMENTS OF AT&T

AT&T Services, Inc., on behalf of itself and its affiliates (together, "AT&T"), respectfully submits these comments in response to the Federal Communications Commission's ("Commission") Notice of Inquiry (*"Notice"*) in this proceeding.[1]

I. INTRODUCTION AND SUMMARY

The early 2010's began what is now an ongoing trend in communications from proprietary closed interfaces towards open network architectures. This shift started in the core of communications networks and is migrating to the radio access network ("RAN"). At the same time, there has been an ongoing consolidation of network hardware and software vendors (i.e., suppliers) that has been particularly acute among those supporting the RAN. This consolidation has led to concerns about the long-term viability and competitiveness of supply chains (and the resulting impact on innovation) and the United States' capacity to keep pace with international rivals.

Open, more modular, RAN ("O-RAN") has the potential to help address those concerns[2] and to unleash more innovation by reducing barriers to entry and opening the industry to more

[1] *Promoting the Deployment of 5G Open Radio Access Networks*, GN Docket No. 21-63, Notice of Inquiry, 86 Fed. Reg. 16349 (released March 18, 2021).

[2] *Id*. at 16350 ("Open and virtualized radio access networks have the potential to address national security and other concerns that the Commission and other federal stakeholders have raised in recent years about network integrity and supply chain reliability.").

competiton and investment. By way of example, when interfaces were standardized and opened in the information technology ("IT") industry, a wide range of companies emerged to provide IT infrastructure. While the communications industry continues to make good progress in its shift toward open networks and its corresponding work through groups like the O-RAN Alliance, the U.S. government can complement industry efforts and make decisions that appropriately set the stage for the future. In short, both industry and the U.S. government can and should invest in the future of the supply chain marketplace to ensure that it develops the requisite scale and offers sufficient opportunities for expansion.

Congress can fund the Utilizing Strategic Allied ("USA") Telecommunications Act authorized last year in the fiscal year 2021 National Defense Authorization Act. The USA Telecommunications Act provides funds supporting research and development and the establishment of a multilateral fund to level the playing field in support of Open RAN. The U.S. government can also play a role internationally by coordinating with our allies policies that support open and interoperable networks.

The Commission also plays a role on many fronts. First, by modifying its rules implementing the Secure and Trusted Communication Networks Act of 2019 ("H.R. 4998")[3] to allow O-RAN as an option to replace covered equipment. Second, through the International Bureau collaborating with other Federal agencies in education and supporting O-RAN with foreign governments. Third, extending its existing Communications Security, Reliability and Interoperability Council ("CSRIC") working group on 5G security to address O-RAN security.[4]

[3] Secure and Trusted Communications Networks Act of 2019, H.R. 4998, 116th Congress.

[4] *See Public Notice*, DA 21-430, FCC Announces Intent to Re-Establish the Communications Security, Reliability, and Interoperability Council and Solicits Nominations for Membership (released April 15, 2021).

This will provide an avenue for the Commission and industry to collaborate and demonstrate security in an "open" environment addressing a common criticism of O-RAN. As Congress appropriates funds for the USA Telecommunications Act, the Commission can serve as part of the advisory board established in the legislation to determine how to best allocate grants. Finally, the Commission can work with other agencies, in particular the National Institute of Standards and Technology ("NIST"), and private sector entities on potential plug fests to showcase and demonstrate interoperable network components.

For its part, AT&T has played a key role in moving the industry towards open network architectures. AT&T is a founder of the Open Network Automation Platform ("ONAP"), which is now part of the Linux Foundation and focuses on creating a "comprehensive platform for orchestration, management, and automation of network and edge computing services for network operators, cloud providers, and enterprises."[5] AT&T also is a founding member of and currently chairs the O-RAN Alliance, whose "mission is to re-shape the RAN industry towards more intelligent, open, virtualized and fully interoperable mobile networks."[6] We are also the founder and currently chair the Open RAN Policy Coalition ("ORPC") and serve on the board of the Open Networking Foundation ("ONF"). Below AT&T provides more specific comments on these and other key issues raised in the *Notice*.

II. DISCUSSION.

A. State of Development and Deployment of Open RAN Solutions.

For several years, the communications industry has been shifting from proprietary closed interfaces towards more open network architectures. Understanding this trend towards open

[5] www.onap.org

[6] www.o-ran.org

communications networks will help identify areas where incentives may be most useful to accelerate development.

1. ***Industry Trend Towards Open Networks.*** Network operators traditionally built networks by interconnecting components that serve different functions, e.g., switches, routers, access nodes, multiplexors, and gateways.[7] Most of these network functions were implemented as integrated and closed systems – unique hardware tightly bundled with equally unique and inseparable software, along with a vendor-specific management and automation system. For operational ease, network operators traditionally used one or two vendors for a given class of network components. And, those vendors became locked-in as the vendor's hardware and software providers because most network hardware components were seldom replaced, resulting in limited options to upgrade as technology advances.[8]

The past decade has signaled a paradigm shift, as network operators with hardware centric networks transform to software defined networks.[9] In this new model, the hardware is standardized and commoditized, supporting multiple network functions through software (i.e., virtual network functions). Network operators can independently select and upgrade the now disaggregated hardware and software to benefit from technological advances. This software-based approach

---

[7] *See National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem*, Appendix A: 5G Case Study (Sept. 3, 2019) ("*NPSTC Report App.*"), available at https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_2.pdf.

[8] *NSTAC Report App.* at A-4.

[9] For example, AT&T's network transformation program has been underway for years. See AT&T, 7 Principles of AT&T's Network Transformation Disaggregation, Cloud, and Intelligent SDN (Q2 2020), available at https://about.att.com/content/dam/snrdocs/7_Tenets_of_ATTs_Network_Transformation_White_Paper.pdf. (last accessed April 25, 2021).

enables a high degree of operational automation, allowing network operators to scale their networks to match demand and ensure maximum utilization of network resources.[10]

This migration to software-defined networks started in the network core. For example, in 2017, more than 50 of the largest network and cloud operators representing 70 percent of the world's mobile subscribers formed the ONAP project to deliver an open, standards-driven architecture and implementation platform. ONAP seeks to rapidly instantiate and automate new services and support complete lifecycle management of software-based virtual network functions. As a result, operators can leverage existing network investments while accelerating the development of a virtual network function ecosystem.[11]

While ONAP's initial efforts focused on network core infrastructure, both the O-RAN Alliance and ONAP lead similar developments occurring in the RAN. The O-RAN Alliance's "mission is to re-shape the RAN industry towards more intelligent, open, virtualized and fully interoperable mobile networks."[12] The wireless RAN is comprised of base stations connected to each other and to the Enhanced Packet Core or 5G Next Generation Core network. These base stations are comprised of multiple components, most importantly the antenna, which propagates radio frequency ("RF") signals; the radio unit ("RU), which transmits, receives, amplifies, and digitizes those RF signals; the Distributed Unit ("DU"), which performs real-time, baseband processing functions; and the Centralized Unit (CU), which performs packet processing functions deep in the network near the core.[13]

---

[10] *NSTAC Report App.* at A-5.

[11] See www.onap.org.

[12] www.o-ran.org

[13] *See* Open RAN Policy Coalition, *FAQs*, available at https://www.openranpolicy.org/faqs/ (last accessed April 21, 2021).

Vendors of traditional RAN hardware and software maintain key connections as proprietary/closed interfaces. For example, in the past a component from Company A (such as a radio) could not communicate with a component from Company B (such as a baseband unit), and individual base stations from one vendor would have limited interoperability with base stations from another vendor. This requires network operators to build networks with fully integrated solutions from a single vendor. Thus, while many operators use multiple RAN suppliers, the operators typically were forced to deploy with a single vendor in a given geographic area.[14]

Opening and standardizing these interfaces and shifting from dedicated proprietary hardware to commodity hardware, all as proposed by the O-RAN Alliance, will allow multiple vendors to provide radio units, baseband units, and backhaul, and network operators to shift to modular networks with different components and software sourced from different vendors. The result will be the potential for much greater vendor diversity.

2. AT&T O-RAN Support. AT&T has played a key role in moving the industry towards open network architectures. AT&T is a founding member, member, and/or serves on the board of multiple organizations supporting the migration towards open networking, including ONAP, the O-RAN Alliance, ONF, ORPC, the Open Infrastructure Foundation, the Cloud Native Computing Foundation, and the Telecom Infra Project. AT&T has extensive experience in constructing lab environments (e.g., AT&T Labs' leadership) and in operationalizing complex network architectures with multiple components, as would be required in an O-RAN configuration. AT&T has also worked on O-RAN pilots and in particular Open Fronthaul (the interface between the RU and the DU) with multiple suppliers including CommScope, Nokia, Intel and Samsung.

[14] *Id.*

AT&T expects to incorporate O-RAN compliant equipment into its network within the next year. The challenge for an operator shifting to any open network architecture, including but not limited to O-RAN, will be maintaining network reliability, integrity and performance for customers during the transition. For our part, AT&T serves multiple customer groups, with varied and often complex, service requirements. As we introduce O-RAN into our network, our goal will be maintaining the same high level of performance at scale. We are actively working in this direction. For example, AT&T recently conducted trials and demonstrations with multiple vendors of an open front haul leveraging O-RAN specifications.[15]

While the industry will likely experience a gradual introduction of O-RAN into existing networks, those developments are not mutually exclusive. Some deployments may still leverage traditional network infrastructure. For example, many 5G RAN deployments will be specific to the site environment or the particular needs of a customer. At the end of the day, the best policies would promote competition among vendors and investments in technology, which will drive the best value proposition in terms of cost, scale and performance. The Commission should encourage

[15] *See e.g.,* O-RAN Alliance, *First Global Plugfest to Foster Adoption of Open and Interoperable 5G Radio Access Networks* (Dec. 19, 2019), available at https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5f88ac86a861db37b8f7df78/1602792591334/O-RAN-2020.10.15-PR-2nd-O-RAN-Plugfest-v1.0.pdf; O-RAN Alliance, *Second Global Plugfest Demonstrates the Accelerated Readiness of Multi-vendor O-RAN Compliant Network Infrastructure* (Oct. 15, 2020), available at https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5dfba8fb1326ae1bcf4a8b6f/1576773884092/O-RAN-2019.12.19-EC-C-PR-on-2019-Plugfest-v1.0.pdf; Bloomberg, *O-RAN Alliance Continues to Grow as Global Operators and Suppliers Reach Across Borders to Collaborate on Open Innovation in Radio Access Networks* (Feb. 20, 2020), available at https://www.bloomberg.com/press-releases/2020-02-20/o-ran-alliance-continues-to-grow-as-global-operators-and-suppliers-reach-across-borders-to-collaborate-on-open-innovation-in; Nokia Press Release, *Nokia and AT&T Run Successful Trial of the RAN Intelligent Controller Over Commercial 5G* (June 18, 2020), available at https://www.nokia.com/about-us/news/releases/2020/06/18/nokia-and-att-run-successful-trial-of-the-ran-intelligent-controller-over-commercial-5g/ (all last accessed April 25, 2021).

those policies that promote such competition and investment and avoid any one-size-fits-all solution or architecture.

B. Potential Public Interest Benefits in Promoting Development and Deployment of O-RAN.

1. Market Growth and Increased Diversity. To be sure, consolidation of the already limited number of RAN vendors presents long-term concerns for the wireless marketplace.[16] The combination of increased competition from purportedly subsidized vendors from China along with consolidation of other vendors has decreased vendor diversity and created challenges for new entrants. Upfront costs related to labor, equipment, and research and development all work to discourage new communications equipment vendors from competing with established players.[17] Yet, the migration towards open networks provides an opportunity for market correction by driving the industry toward a more interoperable, modular network design that will lower barriers to entry, and hence foster competition between vendors. It is critical that the U.S. put in place the right policy framework to allow the technical solutions championed by ONAP, the O-RAN Alliance, and other open network groups to succeed. In effect, those policies would generate a down payment on a more diverse supply chain in the future.

At the same time, mobile network operators are well down the road deploying 5G and cannot cannot change their deployment plans midstream. While the Commission can take steps to help accelerate and lay the foundation for O-RAN, the Commission should avoid taking steps that will distort the marketplace and negatively impact investment or slow down 5G deployments by requiring mobile operators to use particular technologies or vendors. Those actions would

[16] Comments of AT&T Services, Inc., *The National Strategy to Secure 5G Implementation Plan,* NTIA Docket No. 200521-0144 (filed June 25, 2020).

[17] *Id.*

introduce uncertainty into the mix, which is typically detrimental to competition and investment, and may derail the Commission's goals in this proceeding.

2. Open Networks and Security. 5G networks will have improved security and subscriber privacy compared to previous generation networks. Several innovations in a secure network design framework and wireless technology will intersect to create a highly secure and resilient 5G network. Security will also be more agile and layered as we transition from centralized core and radio access networks to distributed, virtual networks. As compute functionality shifts closer to the edge, network operators are implementing new and embedded security functionalities, such as Distributed Denial of Service ("DDoS") detection and mitigation to enhance the ability to respond to attacks and reduce potential broader network impact; stronger encryption for over-the-air interface and encryption of Subscription Permanent Identifier ("SUPI") to further secure communications and protect consumer privacy information; and Security Edge Protection Proxies that mitigate vulnerabilities in prior technologies (e.g., SS7 and Diameter) when subscribers roam between different carriers' networks.

All 5G deployments will benefit from these enhancements. Likewise, 5G uses a service based architecture, a foundational change in mobile architecture that brings flexibility in communication between elements leveraging commonly used HTTP/2 in IT or cloud architecture. This shift enables a range of previously unavailable security controls to be applied in 5G networks. A common principle that can be applied to 5G networks is the concept of "zero trust" networking, meaning anything connecting to a network should inherently not be trusted unless it can be verified. This differs from the traditional closed network architecture concept that relied on security at the perimeter, where a user or device can move freely within a network once it is permitted access.

Zero trust networking can enhance security in a variety of ways by: (a) securing the technology and application stack, including all interfaces and application programming interfaces (APIs); (b) leveraging the cloud-based nature of 5G and deploying cloud security functionality and telemetry; (c) enabling tailored and customized control of security via network slicing; and (d) deploying multiple layers of authentication. The development of these advanced security features and capabilities are underpinned by a robust standards development ecosystem that is facilitating greater security in 5G generally and in areas essential to enabling more open network architectures.

Open architecture has the potential to build upon these 5G enabled security enhancements by allowing a network operator to fully control the security of the network and giving that operator greater visibility to security events. A network operator will have direct access to more data about network performance because the components are disaggregated and connected through open interfaces. This will allow the operator earlier visibility into insights about potential security problems. Data also can be finer-grained and represent activities between/within network functions that were previously hidden by internal vendor interfaces. Further, data about the running state of network functions will be more easily available through open management interfaces. This data can be combined with security log data to drive root cause analysis.

The introduction of open interfaces in the RAN also allows the operator to distribute security analytics throughout the network and move RAN monitoring to the edge. This creates opportunities to create edge-focused analytics that speed the detection and prevention of network attacks, threats, and vulnerabilities and drive closed-loop actions at the RAN, which blocks malicious traffic from reaching the network core. Rapid detection and response can enable efficient and more secure support of mobility services, especially Internet-of-Things (IoT) services, by more effectively preventing DDoS attacks on the RAN by rogue mobile devices. Distributed

security analytics allows an operator to share insights between the RAN and the network core, as well as between different RAN locations. Such insights can be used to take measures that protect RUs adjacent to another RU that is under attack or to use insights about the core to protect potentially vulnerable RUs.

Open networks will also allow operators to integrate best-in-class security platforms with open interfaces defined to be secured using modern, industry-standard security protocols. Since security platform vendors typically provide native support for standard protocols and interfaces, the network operator can integrate new security platforms without having to customize them to fit vendor-proprietary protocols and interfaces. Furthermore, network function vendors will deliver regular protocol updates to stay current with protocol releases, allowing operators to stay current with industry best practices at no extra cost.

Finally, open networks can speed the complete automation of network management. Automation enables zero-touch management, eliminating the security risks inherent in human access to network functions. Such risks include the threat of humans accidentally altering the security posture of a network function or maliciously harvesting credentials, changing configurations, or implanting malware within the network. Automation also increases closed-loop response to changes in the network. For example, by using an open management interface for checking the security posture of a network function, the network operator can quickly detect and fix degraded configurations through closed-loop management. Open networks will also increase the speed with which operators can install software and operating system security patches, thus enabling the operator to minimize the amount of time a vulnerability is in the network.

3. ***Additional Considerations Regarding Open RAN Development and Deployment.*** While Open RAN requires more management in comparison to reliance upon a single vendor, this

can be managed in a variety of ways. Large network operators, like AT&T, typically manage their own environment. Smaller network operators likely can harness systems integration services that will effectively enable operators to outsource management of their complex vendor ecosystem. In regards to security and the heightened risk of using new vendors with shorter track records, this is certainly an issue to consider in choosing vendors. But, our view is that security is enhanced by the inherent flexibility of O-RAN, as explained above. Artificial intelligence and machine learning are also capabilities that can be leveraged with O-RAN to improve security.

On the issue of FirstNet and barriers to adoption by established network operators, the main challenge for an operator like AT&T will be integrating O-RAN with the already massive investments in existing infrastructure while simultaneously maintaining, at scale, the same high levels of reliability, integrity and performance customers expect. AT&T's diverse customer base includes individuals, small businesses, government agencies, including FirstNet, and large enterprise clients, many of which require an extremly complex feature set. AT&T will not introduce new technology that cannot or will not fulfill all of those requirements at scale. More work needs to be done to ensure that O-RAN can meet our complex feature set. AT&T is working with several partners on addressing these issues and fully anticipates resolution over time.

C. Potential Commission Efforts to Promote Development and Deployment.

1. Supporting the Development of Open and Interoperable 5G. The global transition to open and interoperable 5G networks has begun and commercial deployment of O-RAN technologies is expected to ramp up considerably over the next few years. Initial commercial efforts will likely entail greenfield deployments in areas without congestion and that have relatively low performance demands. Over time, O-RAN technologies will evolve to handle the greater performance requirements needed to serve larger and more concentrated areas.

This nascent shift in network architecture presents a particularly important opportunity for the United States, which has typically led the world in developing innovative software-based applications.[18] U.S. leadership on 5G should align with the industry's phased approach to 5G deployment, helping to sustain and encourage competition among existing vendors in the near-term, while encouraging the longer-term transition to O-RAN and open and interoperable 5G networks. Equipment purchases are long-term investments, as equipment is costly to replace. So, even as network operators transition to greater openness, many network operators will continue to use a combination of closed, mixed, and open components for the next few years. For example, AT&T plans to focus on building openness into radio and baseband equipment first, followed by open interfaces in other parts of the network. Meanwhile, newer vendors entering the marketplace must develop the manufacturing capacity to deliver products at scale, allowing them to compete effectively with larger, most established vendors.

Consistent with this phased approach, the Commission can take many of the steps outlined above to help advance O-RAN. As outlined above, this includes making O-RAN an option to replace covered equipment in its rules implementing H.R. 4998; collaborating with other Federal agencies in outreach to our allies regarding O-RAN; extending its existing CSRIC working group on 5G security to address O-RAN security; serving in an advisory role as NTIA implements the programs contemplated in the USA Telecom Act and in working with other agencies, in particular

[18] James A. Lewis, Sr. Vice President and Director, Technology Policy Program, Center for Strategic International Studies, Statement Before the Senate Committee on Commerce, Science, and Transportation, 5G Supply Chain Security: Threats and Solutions, at 6 (Mar. 4, 2020), available at https://www.commerce.senate.gov/services/files/563D903B-FEF0-4A1C-9202-A7DC1CCEFC6F (last accessed April 25, 2021).

NIST, and private sector entities on potential plug fests to showcase and demonstrate interoperable network components.

2. Collaborate with Private Sector in Global 5G Standards and Open Source Software.

Global technical standards set by standards-setting bodies are critical for interoperability among networks and devices.[19] Continued and enhanced U.S. participation in these standards-setting efforts, as well as increased coordination at the regional level through the Alliance for Telecommunications Industry Solutions (ATIS), will ensure that technical standards do not favor any single country's preferred technology, and will support the goals of openness and interoperability.

Many standardization efforts are underway, aimed at different aspects of the 5G ecosystem. The leading organization is the 3GPP, with ATIS as the North American organizational partner. 3GPP developed and is continuing to roll out elements of key 5G New Radio specifications. Equally important are efforts aimed at network openness and interoperability, such as the aforementioned ONAP, the O-RAN Alliance, and the O-RAN Software Community. Government support for the open-source architectures and software these entities are developing will be a key to the success of the open ecosystem and the acceleration of innovation.

In addition to promoting interoperability, standards-setting efforts promote critical cybersecurity efforts. For example, 3GPP has a dedicated security working group, and several other standards bodies and organizations — including the Internet Engineering Task Force (IETF), ATIS, European Telecommunications Standards Institute (ETSI), and Counsel for Securing the Digital Economy — are developing 5G security standards. Participation by U.S. industry and

[19] Patrick Moorhead, *The Crucial Role of Wireless Industry Standards in 5G*, Forbes (Sept. 1, 2017), https://www.forbes.com/sites/patrickmoorhead/2017/09/01/the-crucial-role-of-wireless-industry-standards-in-5g/#626e57ca2cff (last accessed April 25, 2021).

academics, and coordination of U.S. positions in ATIS, is essential to ensure the resulting standards support the goals of a robust, competitive supply chain.[20] 3GPP and other bodies work to ensure regional balance and transparency among participating entities, but maintaining that balance requires broad participation.

Government support and partnership in standards setting efforts is equally important. Government should continue to leverage existing processes towards standards like ATIS, where it works through ATIS and collaborates with the private sector. Government can also play an important role in coalescing industry to determine if there is a need for incentives to ramp-up U.S. private sector representation in standards bodies and if so, to identify the appropriate incentives (e.g., research and development tax credits, direct funding support, etc.). This type of standards support will help solidify U.S. leadership in standards development.

3. Promote Research and Deployment of Open Technologies. Government support can not only support existing vendors, but also advance the transition to openness. For example, as open equipment becomes commercially viable, the United States' purchasing requirements should also evolve to follow the example of private carriers that prioritize those vendors that are committed to open and interoperable networks. For example, the Japanese company Rakuten requires suppliers of new equipment to enable an open radio interface requirement.[21] Also, H.R. 4998, which became law in March 2020, authorized funding to help telecommunications

[20] James A. Lewis, *How Will 5G Shape Innovation and Security: A Primer*, Center for Strategic and International Studies, at 7 (Dec. 2018), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf (last accessed April 25, 2021).

[21] Linda Hardesty, *Cisco's Early Bet on RAN Virtualization Propels Altiostar*, FierceWireless (May 6, 2019), available at https://www.fiercewireless.com/tech/cisco-s-early-bet-ran-virtualization-propels-altiostar (last accessed April 25, 2021).

companies purchase from trusted providers new hardware and software, including "virtual communications equipment, application and management software, and services."[22]

Government can also help spur critical research and development that will have global impacts. Although today's dominant suppliers of RAN equipment are based overseas, the U.S. is a world leader in many of the technologies necessary for interoperable 5G and software-based networks. Tax-free research and development grants to develop advanced network technologies will help build a base of expertise and a pool of U.S.-based suppliers. Support for core open source software concepts will help create a foundation for innovation and commercialization. Government can also provide financial support for foreign vendors to move research and development operations to the United States and develop solutions for the U.S. market**.**

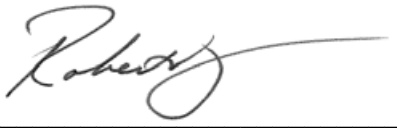
4. Supporting Vendor Diversity Worldwide. The U.S. cannot consider issues related to O-RAN in a domestic vacuum. The aforementioned efforts government can take to help increase vendor diversity domestically can also have global impact. In order to achieve the scale necessary to ensure the market opportunity for new, innovative solutions in the RAN equipment supply chain, these efforts must expand beyond the U.S. Today, many other countries are also considering how to address these concerns, such as the developments that occurred in 2019 around the Prague Proposals. We urge the U.S. government to continue its work with other governments to expand market opportunities and help diversify the supply chain. Such commitments are critical to helping to ensure the necessary scale so that existing and new vendors will flourish.

It is also important that government avoid steps that may hamper or politicize the standards setting process. Some proposals would more directly inject the U.S. government or affiliated entities, such as DOD and NIST, into standards setting as opposed to relying on traditional means

[22] Secure and Trusted Communications Networks Act of 2019, H.R. 4998, 116th Congress.

of influence where they work in concert with industry and through established North American standards bodies such as ATIS. It is important for the future of the industry that standards setting bodies remain private sector led.

Respectfully submitted,

By: 

Robert Vitanza
David J. Chorzempa
David L. Lawson

AT&T Services, Inc.
208 S. Akard Street
Rm 3011
Dallas, Texas 75202
(214) 757-3357 (phone)
robert.vitanza@att.com

April 28, 2021