**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

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

**COMMENTS OF ITI**
**(THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL)**

The Information Technology Industry Council (ITI) appreciates the opportunity to submit a response to the Federal Communication Commission (FCC) Notice of Inquiry (NOI) on *Promoting the Deployment of 5G Open Radio Access Networks.*

ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. ITI's diverse membership comprises companies that operate in almost every layer of the 5G stack, including semiconductor and network equipment designers and manufacturers, software and digital services companies, as well as those that will harness 5G to evolve their businesses.

We have supported the USG's increased focus on enabling the deployment of the next generation of cellular network technology; indeed, 5G will be transformative for our society, offering opportunities to U.S. companies and consumers not previously available. In particular, we were supportive of the previous Administration's efforts to develop a whole-of-government approach to 5G in its *National Strategy to Secure 5G* and Implementation Plan and its focus on promoting the secure development and deployment of 5G globally, with one activity in particular

aimed at developing policies and strategies for global market competitiveness and diversity. We encourage the Biden Administration to carry forth this Strategy. To the extent that the FCC's NOI can help feed into a broader whole-of-government approach to 5G, we welcome the opportunity to provide specific comments on Open RAN, which is one tool that can be used to facilitate greater diversity, innovation and competitiveness.

As a general matter, we support the goal of promoting a competitive wireless market for the Radio Access Network (RAN) based on open and interoperable interfaces as the network transitions to 5G, 6G, and beyond. At the same time, we stress that the best way to maximize the benefits of new technologies is to promote a competitive marketplace and let market forces work. So, it is important that the FCC, and the USG more broadly, support a technology-neutral environment that promotes innovation, allowing the private sector to lead and the market to determine the "winners."

At the outset, we encourage the FCC to clearly indicate what it means when it uses the term "open." We recommend that the FCC clarify that "open" in this context means "supports defined, standardized interfaces among the parts of the 5G stack." In some instances, the use of the term "open" in the Notice of Inquiry (NOI) seems to conflate open architectures with open-source software. While we appreciate the importance of facilitating interoperability across different implementations, we recommend that the FCC clarify that "open architectures" refers to the interfaces themselves, and that the elements of these networks can be built out using anything from open source to proprietary technology in the form of hardware, software, and services.

Below, we offer our thoughts on several of the areas the FCC requests input on. In addition to commenting on discrete aspects of Open RAN deployment, we also offer our thoughts on virtualized RAN (vRAN) as a part of Open RAN systems.

1. **State of Development of Open RAN Solutions**

- *the current state of the standards and specifications development for 5G and Open RAN, including what types of companies are driving the standardization efforts, challenges associated to the standards development process, and steps the FCC can take to address those challenges.*

The NOI rightly notes that several different types of bodies are engaged in advancing the Open RAN model. There are also specific standards bodies that are working to develop the technical specifications that will guide the implementation of open networks, most notably the O-RAN Alliance. The O-RAN Alliance builds upon the technical specifications for RAN architecture developed by 3GPP. The O-RAN Alliance Security Focus Group, formed in March 2020, is now advising the O-RAN working groups to evolve its standards to make O-RAN specific architectural changes more secure to meet the expectations of network operators and their customers.[1]

In our response to the RFC on the Implementation Plan for the *National Strategy to Secure 5G*,[2] we encouraged the USG broadly to support increased U.S. industry participation in standards bodies working on 5G specifications, through supporting industry-led bodies with transparent, rules-based processes; making the United States a more attractive meeting location for standards development organizations (SDOs) to host meetings; ensuring that current and future policies and regulations do not unintentionally inhibit U.S. company participation in international standards bodies; reexamining NISTIR 8074 to see whether and how recommendations are applicable to 5G work; and regularly communicating with U.S. industry.

[1] https://www.o-ran.org/blog/2020/10/24/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components
[2] https://www.ntia.doc.gov/files/ntia/publications/iti-council-0625220.pdf

We reiterate those recommendations here and encourage the FCC to consider them as it determines how it can, in conjunction with others in the interagency, support increased U.S. industry participation in standards bodies developing 5G technical specifications, including 3GPP and the O-RAN Alliance.

## 2. Potential Public Interest Benefits in Promoting Development and Deployment of Open RAN

*The effect of Open RAN on market entry, vendor diversity, and competition in the wireless network equipment industry.*

Over the last few decades, the market for telecommunications equipment has undergone a consolidation, particularly in the radio access network equipment sector. Open RAN is one technology solution which the United States could leverage to address some of the challenges related to vendor diversity that have emerged due in part to this consolidation. Using open, interoperable standards means that networks can be built more easily with multiple vendors, which in turn helps to foster new market entrants and competition. With increased competition, companies are incentivized to innovate and develop the best technology solutions. A key goal of Open RAN is software virtualization to enable cloud-based deployments, though it is important to note that this goal is also achievable with vRAN and Cloud RAN.

*To what extent Open RAN addresses supply chain risk management issues and enables the deployment of secure and reliable networks in the U.S.*

There are many threats to the supply chain today. In fact, the ICT Supply Chain Risk Management Task Force Threat Evaluation Working Group has identified 188 supplier-related

threats, including "reliance on single-source providers."[3] Open RAN can address one discrete aspect of supply chain risk – that associated with vendor diversity specifically in the radio access network. A radio access network built on a diverse vendor base reduces the reliance on a single vendor, mitigating the potential risk associated with vendor lock-in. Importantly, as with the other 187 threats identified by the Task Force, threats related to Open RAN should be viewed and can be managed through the lens of risk management. So, on the one hand, Open RAN can help manage supply chain risk associated with vendor diversity, but on the other we should remember it was not explicitly developed for the purpose of addressing discrete cybersecurity supply chain challenges.

For instance, Open RAN can introduce supply chain risk that vendors should be aware of and seek to manage. While not all Open RAN deployments utilize open-source software (OSS), to the extent that they do, vendors should ensure that they utilize solutions containing open source code with proper due diligence (just as they should with respect to managing vulnerabilities in proprietary software) so as to ensure that vulnerabilities are not unintentionally or maliciously introduced and then propagated via software. The O-RAN Alliance's Security Focus Group (SFG) will be producing guidelines for its members so that they are able to securely leverage open-source code.

We offer additional considerations related to the cybersecurity threats and opportunities presented by Open RAN under subheading (3).

[3] https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf

*Specific thoughts around the technological benefits of Open RAN deployment.*

As we note in our 5G Policy Principles and 5G Essentials for Global Policymakers,[4] the way in which telecom networks are built is evolving, shifting away from legacy telecommunications systems to an information-technology based infrastructure, leveraging technologies like the cloud. In our 5G Essentials, we highlight several key emerging information and communications technologies that are driving the deployment of 5G, including solutions like network functions virtualization (NFV).

Virtualization separates the network functions from hardware on a network and allows them to be managed through virtual machines, including through cloud-based solutions. This presents the opportunity for software applications to be run on widely available hardware, allowing for more flexibility than in previous generations of telecom networks. In the context of the RAN, virtualization can help enable operators to meet quick time-to-market demands; increase compute power, networking storage, and security requirements; enable automation, Artificial Intelligence (AI) and Machine Learning (ML); and enhance network security options.

One of the goals of Open RAN deployments is to leverage software virtualization for deployment in the cloud with orchestration and automation for efficient and agile use of resources, a goal that can also be achieved with 3GPP-specified RAN architectures deployed as vRAN or Cloud RAN.

While the evolution to O-RAN networks that match the security, resiliency, and performance of today's networks may take a bit longer, Open RAN using vRAN and Cloud RAN technology will be deployed in networks sooner. Using Open RAN may also help to address

[4] https://www.itic.org/policy/ITI_5G_Full_Report.pdf

pockets of the network that seem to linger when there is a transition to the next generation or where other technologies have been slow to rollout.

### 3. Additional Considerations Regarding Open RAN Development and Deployment

We appreciate that the FCC is considering multiple questions related to Open RAN development and deployment, including related to the security of such an approach. The NOI asks two questions related to risks and vulnerabilities that Open RAN might introduce, or that operating in a virtualized environment may introduce. Below, we offer perspectives on each.

*Whether Open RAN could introduce new vulnerabilities and whether openness introduces new risks to the network.*

Open RAN-based networks have many of the same cybersecurity challenges as traditional RAN-based networks. Security threats and risks such as malware, botnets, command-and-control (C2), and other forms of attacks are potential risks regardless of the underlying architecture. In addition, regardless of whether the access network is a traditional RAN or Open RAN, the RAN's connection to the core of the network (the backhaul) is the same. It is important that connection is secured by leveraging full visibility of the threats and real-time prevention mechanisms to stop cyberattacks, based on automation. At the same time, while O-RAN architecture can create an expanded threat surface, work is currently underway to ensure the security of additional O-RAN interfaces and functions. This is an area that the O-RAN Alliance SFG is working on – it has set work items that are aimed at better securing the O-RAN Open Fronthaul Interface, Near-RT-RIC and third-party xApps, certificate-based authentication with PKIX on management interfaces and untrusted links, and use of open source code.

Whether they incorporate Open RAN-based solutions or not, network operators will need to take a risk-based approach to managing the security of 5G networks, which in some cases may include developing and executing a plan to leverage sophisticated, enterprise-grade security. Whereas to some extent any novel innovation to 5G networks, including Open RAN-based solutions, may mean there are additional security considerations to be managed, Open RAN-based architectures also provide significant opportunity for building increased security features into the network, including by leveraging virtualization and network segmentation.

*Risks associated with a virtualized operating environment*

In many cases, operating in a virtualized environment may actually help to enhance security. A core component of 5G is the cloud-native fabric. This allows for additional security enhancements and capabilities. For example, it facilitates the rapid deployment of infrastructure and services. This is done via incorporating leading security practices and standards into the development lifecycles to address operator requirements, integrating zero-trust architecture, and using cloud services as a catalyst to further security innovation, employing IoT, big data, and AI/ML. It also allows for greater visibility into threats and security telemetry, while facilitating a scalable and dynamic approach. Networks built on open and interoperable standards in particular, allow for greater transparency into the lifecycle process.

Beyond this, security capabilities and services are continuously created and deployed to secure cloud architecture. Ultimately centered around a zero-trust approach and a secure development lifecycle, cloud security capabilities are distributed across the lifecycle, including during the “build” stage, when developers are pushing code into the cloud, as well as during the

operations and maintenance stage. Cloud security uses practices that support security assurance and compliance requirements across the entire lifecycle of these services. This helps operators and enterprises alike build highly secure software, address security compliance requirements through automation, and reduce development and deployment costs. It also includes elements such as vulnerability management processes to periodically scan and validate services. Leveraging cloud-native services also unlocks automated security compliance capabilities across the product lifecycle from procurement to sunsetting to support operators. Finally, cloud capabilities also deliver enhanced platform security by integrating NIST SP 800-193 – Platform Firmware Resiliency Guidelines into 5G edge deployment.[5]

### 4. Potential Commission Efforts to Promote Development and Deployment

*Whether the FCC should enact rules to promote reliability, interoperability, and adoption of Open RAN.*

As we note at the beginning of our submission, Open RAN can certainly help to address some of the challenges that have been identified as the United States and nations globally seek to deploy 5G. We recognize the immense value that Open RAN can bring, especially in allowing for increased innovation and flexibility. While it is important that the USG support a technology-neutral approach, the FCC should play a role in educating operators about the various solutions available, including Open RAN. The best way to maximize the benefits of new technologies is to promote a competitive marketplace and let market forces work. This will allow the private sector to lead and the market to determine the "winners." While we believe that the FCC should explore

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

Open RAN as a viable solution and promote it as a realistic alternative, we discourage the FCC from mandating the adoption of Open RAN.

We also note that while the NOI suggests Open RAN will bolster the competitive advantage of U.S. companies over "traditional network equipment vendors," we believe that the FCC, as a part of broader U.S. policy, should expressly advance a diverse, trusted market of suppliers based in the United States as well as in allied and other partner market democracies. Only a multinational, diverse vendor base of trusted suppliers will have the capacity to service the U.S. and other partner countries' markets.

*Whether the FCC should have a role in promoting/developing/testing Open RAN equipment.*

It makes sense for the FCC to have some role in R&D related to Open RAN equipment. We have stressed on multiple occasions the importance of allocating additional R&D funding to exploring open and interoperable networks, as well as associated 5G use cases. Investments in 5G infrastructure and next generation applications are absolutely imperative in fueling a cycle of investment and innovation. As more consumers and businesses harness 5G, application developers are incentivized to create innovative new offerings. From there, these new applications and use cases drive demand for 5G-enabled devices and connections, thereby encouraging further investment in 5G infrastructure. Examples of R&D and pilot projects that could harness 5G built on open and interoperable infrastructure include innovations in energy monitoring on the power grid and smart network monitoring in commercial facilities that require a high degree of government regulation and security.

To the extent that the FCC can play a role in facilitating pilot projects or testbeds in conjunction with other agencies, we believe this will be helpful to realizing the full potential of Open RAN. As the FCC engages stakeholders and other agencies, it should support making more funding available for test beds and pilot projects.

**5. Commission Outreach, including International Engagement on Open RAN**

*How the Commission can ensure that it does not duplicate efforts with other agencies or contribute to ongoing initiatives, including helping to facilitate industry input into these initiatives.*

As a general matter, one way in which the Commission, and the USG more broadly, can address issues related to duplication of efforts regarding Open RAN is to adhere to the Implementation Plan that was developed as a part of the previous Administration's *National Strategy to Secure 5G.* To the extent the FCC can encourage continued implementation of the *National Strategy* and Implementation Plan[6]*,* this will help to ensure a coordinated, whole-of-government approach to 5G, and Open RAN in particular. A strategic approach, where efforts are streamlined, is essential for the rapid deployment of 5G in the United States and globally.

Under the Implementation Plan, the FCC is listed as a supporting agency for many of the outlined activities. As the USG seeks to implement each activity under the various lines of effort, the FCC should ensure it is actively plugged in and working with the lead and supporting agencies, communicating upcoming opportunities and planned engagements so that other agencies can be made aware and also provide relevant input or context as appropriate.

[6] https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf

For example, activity 4.1 directs the State Department to lead diplomatic engagement with international partners on a variety of 5G issues, and the FCC is tasked with supporting this effort in tandem with other agencies. To the extent that the FCC is participating in international conversations, such as those taking place in APEC or in the OECD or other multilateral fora, it should ensure that its messaging is aligned with diplomatic engagement efforts developed under this prong.

We also encourage the FCC to actively participate in activity 1.1, which is focused on improving research, development, and testing to reach and maintain United States leadership in secure 5G and beyond. As we mentioned in our comments above, we believe that the FCC should play a role in facilitating research and development and so working with others in the interagency on the areas outlined in Annex A, specifically on leveraging existing public-private partnerships through existing USG 5G testbeds and field locations, is something we support.

Finally, we encourage the FCC to also support NIST in carrying out activity 4.4, which is focused on promoting United States leadership in international standards development for 5G, including through private sector and international engagement. Part of this effort should focus on removing barriers to participation for private sector companies, as we reference earlier in our comments (see Section 1, p.2). This will help to ensure that there is adequate private sector representation in relevant standards-setting bodies.

*How the Commission should feed into international Open RAN efforts, including fora it should participate in, information it should disseminate, ways it can encourage stakeholder participation etc.*

As referenced above, we appreciate that the FCC is already participating in multilateral fora on conversations related to Open RAN[7] and would encourage the agency to continue such engagement. APEC is one forum which the FCC should continue to leverage, particularly on conversations related to best practices for 5G security and/or Open RAN more generally. As it brings together 21 economies, APEC is a good forum for disseminating relevant information and learning about what other economies are doing in this space. The FCC should coordinate closely with the State Department as well as ITA and NTIA, who are leading the development of principles for open and interoperable networks to figure out how to best utilize multilateral fora to disseminate those principles once finalized. The *Implementation Plan* also highlights other key fora which the USG should seek to engage in order to encourage the use of trusted vendors, including the North Atlantic Treaty Organization (NATO), the Organization for Economic Cooperation and Development (OECD), and Association of Southeast Asian Nations (ASEAN). These fora may also be good for the FCC -- in conjunction with other agencies as they seek to implement the National Strategy to Secure 5G in a coordinated manner -- to leverage to discuss Open RAN and share information related to opportunities, challenges, costs, benefits, security considerations, and any other relevant information that is collected in response to the NOI.

We also appreciate that the FCC is seeking to ensure that industry remains engaged in international conversations while also promoting industry participation in international fora. We encourage the FCC to regularly communicate with industry about international engagement opportunities that it becomes aware of or that it is participating in.

[7] *Notice of Inquiry on Promoting the Deployment of 5G Open Radio Access Networks*, 78, p. 29.

6. **Costs and Benefits of Open RAN deployment, including for 1) mobile network operators, 2) the costs associated with deployment and interoperability, and 3) the costs and benefits of Open RAN on the broader economy.**

Open RAN deployment can help mobile network operators benefit from multiple vendors in what has traditionally been a single vendor selection. Vendors utilizing Open RAN thus helps open competition in the last mile of the mobile network where competition has not been supported (because of closed systems). Whenever there is competition, there is a cost savings to the buyer. There is also increased resilience and agility that comes with a move towards virtualized networks, including Open RAN networks. A software-defined environment not only offers best in class solutions but allows for rapid iteration and innovation. Currently, providers are generally reliant on a single proprietary vendor for updates to the RAN software. Moving to a virtualized, software-defined Open RAN architecture not only creates the incentive for new market entrants – and vendor diversity— but can also provide the opportunity for constant, swift updates that may introduce new features or functions, condensing the time it takes to upgrade a system.

As with any kind of virtualization, integration is key. This integration has traditionally been left to the vendors themselves, who promote the use of proprietary systems to ease integration. However, this is not unlike any other IT deployments. Anytime a network with multiple applications and services is built in IT, integration is a key component. 5G introduces the opportunity for integrators to get engaged and fill this gap as they traditionally would in any other IT deployment. As such, we are seeing a healthy shift in the roles of suppliers and integrators.

5G deployment also offers opportunities that go beyond traditional telecommunications networks, like private 5G networks. There are only some 800 mobile operators in the world, which is not a big market for new entrants. However, because 5G is not simply the next evolution of mobile technology, it does not matter what the access type is (cellular, satellite, WiFi, and fiber are supported). Private 5G networks are already being built, and when an enterprise wishes to build its own private 5G network, Open RAN technology can be a good solution. An enterprise likely would not be able to afford a traditional RAN based on existing technology, and so introducing a new approach to RAN to support this enterprise market increases the market size tremendously and provides a more viable marketplace for new entrants to survive.

***

We appreciate the opportunity to provide feedback in response to this NOI. Open RAN will be one technology solution that can help to support a competitive, innovative market for RAN equipment, as open and interoperable interfaces will allow for increased agility and flexibility. We welcome continued collaboration with the FCC as it considers how to effectively promote Open RAN solutions.

Sincerely,

John S. Miller
Senior Vice President of Policy
and General Counsel

Courtney Lang
Director of Policy

April 28, 2021