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 MICROSOFT CORPORATION

TABLE OF CONTENTS

I. OVERVIEW

Microsoft Corporation (Microsoft) respectfully submits the following comments in response to the Federal Communications Commission's (FCC or Commission) Notice of Inquiry on Promoting the Deployment of 5G Open Radio Access Networks (NOI).[1] Microsoft appreciates the Commission seeking comments on the development and potential of Open Radio Access Networks (Open RAN).

Microsoft agrees with the comments filed by the Open RAN Policy Coalition (ORPC) detailing the significant public interest benefits of Open RAN, including driving increased competition, innovation, vendor diversity, improved security, and increased affordability. While Open RAN represents a great step towards meeting these goals, it must be accompanied by a holistic view of next generation networks including cloud native approaches and edge computing. An understanding of the role of the cloud in the Open RAN and 5G network is important if policymakers are to successfully define policies that support the emergence and successful evolution of the network.

As the FCC focuses on enabling the buildout of secure and innovative next generation wireless networks, Open RAN will play an important role. As discussed below, the cloud is essential to realizing the full potential that Open RAN presents. Cloud fundamentals of open interfaces bring an ever-expanding ecosystem of developers to strengthen security practices and utilize the best of artificial intelligence and machine learning in the transformation of wireless networks, for this era, and the next. When Open RAN is combined with the cloud, there can be an ecosystem that is vertically and horizontally diverse, providing network operators with a

[1] *Promoting the Deployment of 5G Open Radio Access Networks*, Notice of Inquiry, __FCC Rcd___(2021). (NOI)

larger pool of suppliers and more methods to modernize and secure their networks.

The FCC is properly focused on policies for next generation wireless networks (5G and beyond) that promote security and innovation. In these comments, Microsoft discusses the roles of Open RAN and the cloud, as well as actions the FCC can take.

- To reach its full potential, Open RAN must be paired with cloud capabilities. This will occur in stages, with greater use of the cloud in later stages.
- Cloud technology accelerates security innovation and is proven through industry adoption of best practices and capabilities for security. Open RAN security will depend on cloud security. Cloud security is based on international security and risk management standards, coupled with unparalleled access to security telemetry and integrated Artificial Intelligence (AI) capabilities to prevent, detect, and respond to old and emerging threats across the network, and across the software and firmware supply chains.
- Open RAN will rely on Open Source as well as proprietary software. The use of Open Source Software will yield additional vendor diversity and, when deployed properly, the potential for increased security.
- The FCC has an important role to play and can take specific actions to support the next generation of wireless networks. These specific actions include: adopting technology neutral policies that promote next generation solutions, such as cloud and Open RAN; reimbursing operational as well as capital expenditures; promoting security best practices; providing incentives for rural carriers to improve security; encouraging industry certification; supporting research and development, including test beds and plugfests; partnering with and learning from allied countries; and

assisting with the building of a skilled workforce to help create the next generation of wireless networks.

II. INTRODUCTION

Today, networking and computing are everywhere, embedded in devices we hold in our hands and distributed across wide areas of the country in smart cities, farms, manufacturing sites, and schools. Advances in the cloud, both in the core and at the edge of the communications network, allow for the connection of billions of devices, remote work, greater efficiency, and applications growing at massive scale.[2] Processing power can be distributed to where it is needed most, while maximizing performance and minimizing latency. The cloud can provide colossal amounts of computing power, be accessed from anywhere there is broadband available, and can store huge volumes of data. The cloud can deliver operational efficiencies to businesses across every industry by leveraging next generation wireless networks, including 5G.

With increased numbers of individuals working and connecting remotely, there is a heavier dependency on the cloud to provide services and empower people. The pandemic increased remote education and the consumption of entertainment at home. These services, applications, and content reside in and are managed by the cloud. Customers expect an always-on, mobile-connected experience from their communications service providers as a link to work, family, and friends. As many workers, families, and consumers have been forced to live their lives virtually, Microsoft is seeing significant demand for cloud services resulting in years of digital transformation occurring in mere months.

Looking ahead, communications service providers and network operators (operators) are

[2] In these comments we use cloud to refer to all types of the cloud, whether, private, public, or hyperscale. Microsoft offers all of the aforementioned and anticipates operators implementing Open RAN will use a combination of private, public, and hyperscale cloud offerings.

facing rapid transformation as they undertake the evolution to 5G mobile networks. 5G will allow connection density – that is, significantly more devices will be connected to communications networks and the cloud. This evolution has the potential to digitally transform a diverse set of industries including manufacturing, retail, agriculture, and more.[3] For example, AI-powered decision support tools can assist physicians in making faster and more accurate diagnoses, thereby improving patient outcomes.[4]

While 4G and broadband each created tremendous value in the consumer space, 5G and enhancements in cloud computing will create similar value within the enterprise market. Computing power can now be delivered to the edge of the network as well as directly to enterprises. 5G will provide low-latency connectivity to autonomous vehicles and devices, support high-density sensory devices for the industrial Internet of Things (IoT), and enable the deployment of advanced private mobile solutions. These solutions will be targeted at specific industries: operators will help advance the agricultural industry, enabling farmers to take data from sensors, drones, and satellites to understand precisely how soil, weather, and management intersect; connected smart buildings will enable inhabitants to use the power of mixed reality, interacting with their environment and navigating spaces like never before; and in

[3] *See Connected World: An evolution in connectivity beyond the 5G evolution*, McKinsey, (Feb. 20, 2020). Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/connected-world-an-evolution-in-connectivity-beyond-the-5g-revolution; Cruz, L., *5G technology will enable $13.2 trillion of global economic output by 2035,* Analyst Opinion, Omdia, (Nov. 15, 2019). Available at: https://omdia.tech.informa.com/OM005180/5G-technology-will-enable-132-trillion-of-global-economic-output-by-2035 (Cruz 2019).

[4] *See* Cruz 2019; *Impacts of 5G on productivity and economic growth,* Working Paper, Australian Government, Bureau of Communications and Art Research (Apr. 2018). Available at: https://www.communications.gov.au/departmental-news/impacts-5g-productivity-and-economic-growth

manufacturing, businesses will create digital twins of factories, applying new insights to drive better products, reduce costs, and enable lights-out operations to function during critical times.

While the 5G service-based architecture already defines how network functions can be deployed in the cloud, many of these opportunities will only be unlocked if the ultra-low-latency, highly programmable characteristics of 5G networks can be seamlessly and securely integrated with cloud services and made readily available to a large and diverse community of software application developers.

By leveraging a secure and intelligent cloud, and cutting-edge capabilities enabled by Artificial Intelligence and Machine Learning (AI/ML), the United States and its allies can take leadership in accelerating a global digital transformation. Open RAN, by creating the open interfaces between all the necessary components, is an important element of this transformation.

III. MICROSOFT'S VISION

Microsoft is building a carrier-grade cloud delivering solutions in the core of the network and bringing more Microsoft cloud technology to the edge of the operator's network with our Azure for Operators Initiative. By making the power of Microsoft Azure's hybrid cloud and rich portfolio of cloud services available to operators, Microsoft is committed to working with, not disintermediating, operators. Indeed, partnering with operators is key to connecting the intelligent edge with the intelligent cloud and to creating new transformative experiences for people and organizations everywhere, across every industry. We are also partnering with a number of network equipment providers to offer solutions, including in the Radio Access Network (RAN), that interoperate with the Azure for Operators technology. Open RAN will offer the benefits of easier interoperability, deeper integration, faster time-to-market, and the ability to integrate the power of big data and AI into the more efficient operation of the RAN.

Microsoft seeks to partner with operators, vendors, developers, and creators to build a cloud and network ecosystem that will support innovation by:

- Bringing the **power of the cloud to the edge**: New solutions at the network edge offer step-change advancements in cost, speed, and security, enabling operators to serve customers with new low-latency compute applications.

- Taking an **ecosystem-wide approach**: Platforms such as Microsoft's Azure for Operators bring the scale of the developer and partner ecosystem across everything from network functions to AI, exposing new use case capabilities and **spurring innovation.**

- Helping to **reduce costs and increase revenue**: A software-based, cloud-native alternative to traditional hardware reliant network infrastructure will reduce the cost of providing communications services and allow for increasingly sophisticated end user experiences and services.

- **Integrating sophisticated and intelligent security**: Using cloud as a platform for Open RAN and Open Source software helps operators secure their networks from the start by deploying well established zero-trust principles along with best in class capabilities to defend against cyberthreats.

- **Leveraging Machine Learning and Artificial Intelligence:** The benefits of AI/ML yield the ability to: (1) program the network to improve operational and network efficiency by gathering and stitching together information to produce real-time insights into network health; and (2) automate security defenses to prevent, detect, and respond to attacks.

The building blocks of this ecosystem, Open RAN and cloud native technologies, are interdependent. As such, neither can be minimized when contemplating the next generations of wireless networks.

IV. OPEN RAN, A COMPONENT OF NEXT GENERATION WIRELESS NETWORKS, WILL RELY UPON THE BENEFITS OF THE CLOUD

The evolution toward Open RAN is a further step towards reaping the benefits of virtualization and the cloudification already in progress in next generation wireless networks.[5] In this section we detail: (1) the anticipated evolution of next generation networks; (2) the role of Open RAN in conjunction with a cloud architecture; (3) the role of edge computing; and (4) Microsoft's role as a partner with operators and network equipment providers on the journey to next generation networks.

A. The Stages in the Path to Next Generation Wireless Networks

Nearly a decade ago a whitepaper published by several global operators highlighted the benefits, enablers, and challenges of Network Function Virtualization (NFV) for wireless networks.[6] While virtualization was not new to IT in many sectors, operators saw a potential for greater application in telecom by decoupling hardware and software, leading to lower capital expenditures, and faster deployments. Operators migrating to the cloud will each move at their

[5] 5G is, by definition, "cloud native" meaning the service leverages the approach of building applications and services for the cloud. For instance, the networks can use cloud techniques including Open API, Control-User Plane Separation, Microservices, Continuous Integration and Delivery, and Virtualization. *See 5G and the Cloud*, 5G Americas, White Paper (Dec. 2019) p.39. Available at: https://www.5gamericas.org/5g-and-the-cloud/.

[6] *Network Functions Virtualization*, SDN and OpenFlow World Congress White Paper, (Oct. 17, 2013). Available at: https://portal.etsi.org/NFV/NFV_White_Paper2.pdf. Contributors include: AT&T, CableLabs, Century Link, Deutsche Telekom, Orange, Softbank, Sprint, Swisscom, Verizon, and Vodafone.

own pace, but many will move through three distinct stages.

In the first stage, operators deploy virtualized software solutions in the core of their network, and then seek to partner with public cloud providers at the edge of the network or the edge of the enterprise. Today, Microsoft provides more than 100 commercial mobile operators with virtualized packet core implementations and more than 400 with virtualized voice service infrastructure, indicating a growing presence of convergence for mobile operators in this stage.

In the second stage, operators will move select network functions, often those most easily centralized, to the cloud. Here, leveraging virtualized or containerized network functions in the cloud results in improved security, reduction of costs, increased efficiency, and simplification of the management of more traditional, hardware-based legacy services, such as messaging, or specific voice applications. Many of Microsoft's mobile operator customers are already in this phase.

Open RAN is critical in the third stage. As the network edge adopts cloud technology and cloud vendors continue to extend their infrastructure to the edge, operators will focus on deploying sophisticated access technologies like Open RAN and handle real time traffic “at the edge” for compute-intensive, low latency applications.

B. The Role and Benefits of Open RAN

Having an Open RAN is a foundational component in evolving next generation networks to realize the benefits of the cloud. Open RAN further increases access to critical components -- allowing for more interaction among the virtualized and disaggregated portions of the RAN – yielding greater opportunities for innovation, more offloading to the cloud, and bringing together a diverse ecosystem for a common purpose. RAN components will yield additional benefits, including opportunities for further innovation and enhanced security.

1. Open and Standard Interfaces Lead to Innovation and Security

As operators move through the stages of modernizing wireless networks, steps have been taken to develop standardized interfaces to permit the use of interoperable hardware and software components from different vendors. For instance, the O-RAN Alliance created specifications for the interfaces, or Open RAN, between certain components that traditionally were housed in proprietary hardware in RAN base stations.[7] The opening and standardization of the interfaces will also:

- Enable the creation of a new ecosystem that can bring innovation by sharing RAN information through interfaces in a manner similar to the use of Application Programing Interfaces (APIs) today. Having this information open and available enables the development of new value-added services, such as optimizing power consumption. From Microsoft's long support of APIs, we recognize the power of a rich partner ecosystem of application developers, who can continue to innovate when given opportunities like Open RAN.
- Improve RAN efficiencies by utilizing information collected by AI and ML techniques to address concerns of network congestion and providing better management of the overall network.[8] For example, RAN Intelligent Controller (RIC) is an element that can be used to optimize the performance and efficiency of the RAN by way of AI/ML.[9]

[7] *See* O-RAN Alliance O-RAN Specifications. Available for download: https://www.o-ran.org/specifications (O-RAN Specifications).

[8] *See Open RAN Policy Coalition Comments*, Docket 21-63 at Section II B. (ORPC Comments)

[9] *See* O-RAN Specifications.

- Enhance security by expanding the number of parties examining the interfaces and leveraging AI and ML to address threats and bugs more quickly, as further described in Section V, below.
- Enable easier and more cost-effective RAN sharing by ending dependence on proprietary hardware. Operators currently share infrastructure such as towers to reduce operational costs.[10] Open RAN can provide additional substantial savings for the operators by enabling operators to share more of the infrastructure components, including the RAN.[11]

2. Open RAN Enhances Performance and Scale Through the Virtualization of RAN Components

Microsoft strongly believes that virtualization of RAN is needed to enable operators to meet the growing demand 5G networks place on compute capacity, networking, and storage resources. Virtualization also helps decrease time-to-market. Virtualized implementation of Distributed Units (DUs) and Central Units (CUs)[12] will provide further scaling and performance benefits and lower costs for operators.

---

[10] *Mobile Infrastructure Sharing*, GSMA (2012) at p13-14. Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2012/09/Mobile-Infrastructure-sharing.pdf#:~:text=RAN%20sharing%20is%20the%20most%20comprehensive%20form%20of,at%20the%20point%20of%20connection%20to%20the%20core.

[11] GMSA 2021 Paper at p 10.

[12] The FCC defines a Distributed Unit as the component that manages the radio link, data link, and digital portions of the physical layer of the network, and controls coordinated multi-point and fronthaul capabilities among multiple Radio Units and a Central Unit as the component that oversees the radio resource control and packet data convergence protocol layers of the network, controls multiple Distributed Units over mid-haul interface, and facilitates network traffic load balancing among Radio Units. *See* NOI para 6 and Appendix A containing Figure 1 from the NOI.

3. Open RAN Enables a Diverse Vendor Ecosystem

Open RAN enables increased network vendor diversity by virtualizing and disaggregating network components. New vendors benefitting from a lower cost of entry to the network vendor ecosystem can play a role in developing individual network components, instead of only having the option of producing proprietary bundles of products for operators.[13]

The diverse vendor ecosystem enabled by an Open RAN paired with cloud will allow operators to choose the best-in-class vendors for each network function, avoid vendor lock-in, accelerate innovation coming from a vibrant vendor ecosystem, and drive deployment costs down.

C. The Role and Benefits of Edge Computing

Edge computing, which is needed for massive scale Open RAN deployments, is another important component of next generation wireless networks. Edge computing is the movement of computing closer to where applications and services operate. Moving computing closer to the user of the application supports applications that are highly time sensitive and require very low latency.

As more aspects of the RAN become virtual, the edge has become divided into "near edge" and "far edge" elements. Near edge elements include those parts of a RAN that are located closest to an operator's facilities or cloud data center. Far edge elements sit closer to end users yet remain controlled by the operator.

A disaggregated and virtualized RAN enables operators to distribute Open RAN functions across cell sites, near and far edge, and the central or regional cloud. Centralizing some aspects of RAN functionality increases efficiency and lowers costs. Operators can leverage energy-

[13] *See* ORPC Comments Section II A.

efficient algorithms of cloud platforms and improve failover scenarios across servers. Because the RAN functions are disaggregated,[14] for example into the DU and the CU, this centralization can be achieved for less-latency sensitive applications while still maintaining the most latency sensitive functions at the far edge. Real world deployments will have varying architectures based on their practical needs; distributed open and virtualized RAN gives operators the flexibility to optimize networks depending on the unique needs of a particular deployment.

D. Microsoft will Support Operators Throughout All Stages of This Journey

Many service providers are in different stages of deploying virtualized solutions and 5G networks. As such, they will have diverse needs. Each operator will have its own requirements for reliability, resiliency, security, and performance. First and foremost, operators need a cloud that allows them to retain control over the critical network functions of their choosing while providing easily available programmable interfaces for application developers who can accelerate the ecosystem and innovation. From a cloud that can scale to accommodate billions of connected devices, operators can then deliver ubiquitous computing power, minimize latency concerns, and bring their services as close to the customer as possible. Having a cloud that can accommodate a complex ecosystem of equipment and software vendors, business partners, and network architectures that comprise their solutions today, operators can be more agile for 5G, 6G and beyond. Finally, using hybrid cloud solutions[15] – clouds that recognize that telecommunications functions are distributed throughout the network from the core to the edge – operators can better ensure the high resiliency and security necessary to support critical national

[14] *See* Appendix A.

[15] A hybrid cloud is a type of cloud computing that combines on-premises infrastructure—or a private cloud—with a public cloud. Hybrid clouds allow data and apps to move between the two environments. *See Public Cloud vs Private Cloud vs Hybrid Cloud*, Microsoft Azure available at: https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/

infrastructure.

Microsoft is experienced in providing such a cloud. Microsoft Azure has more than 170 network points of presence (POPs), more than 20,000 peering points, and handles more than 30 billion packets per second. Given Microsoft's depth of experience and with more than 6 billion devices using our IoT services, Microsoft understands the challenge of scaling to meet the demand for a massive IoT ecosystem. Furthermore, Microsoft is able to provide unique insights on the AI and ML technologies that will drive the next generation of 5G applications—already processing more than ten billion AI transactions per month and more than one million machine learning experiments. Microsoft's strong commitment to security enables us to provide operators with a secure and innovative cloud that meets their needs.

Microsoft is committed to working with operators as a partner, not as a competitor. Microsoft is a platform company with the mission of empowering others to achieve more via the use of the cloud, Open RAN, and edge computing.

V. OPEN RAN, COUPLED WITH CLOUD, ELEVATES 5G SECURITY

Cloud is a core enabling technology for Open RAN. Microsoft joined the O-RAN Alliance to work across industry and bring our expertise to contribute to the interface specifications in a way that incorporates cloud security, resiliency, transparency, and trusted solutions to operators. Open RAN's reliance on cloud enables the deployment of secure infrastructure and software across a multi-vendor environment. This enables vendors in Open RAN to readily adopt 5G security and resiliency advantages while mitigating and defending against evolving risks. Microsoft's cloud security enhances the Open RAN ecosystem in several key ways, including: (1) the integration of leading security standards and capabilities; (2) unparalleled access to security telemetry to detect threats; (3) our commitment to delivering enhanced platform and

firmware resiliency from data centers to the far edge; (4) integration of next-generation supply chain security risk management practices and technology solutions; and (5) support for the open source security ecosystem.

A. Cloud Elevates the 5G Security Baseline Through Standards and Advanced Capabilities

To start, Open RAN's reliance on cloud means the baseline for security, privacy, and compliance is elevated across a diverse vendor base. At Microsoft we integrate leading security engineering practices, secure software development standards, and operational security capabilities across our suite of infrastructure and services. For example, Microsoft uses zero-trust principles to enhance resiliency against sophisticated attacks by deploying least privileged access and network segmentation to prevent unintended access and lateral movement across sensitive networks. Furthermore, as a leading software provider, Microsoft applies our Security Development Lifecycle and other software assurance practices in alignment with the National Institute of Standards and Technology's (NIST) Secure Software Development Framework and SAFECode's leading software practices to further enhance software security.[16] 5G's inherently modular nature and recent advancements in software-defined networking (SDN) and network functions virtualization (NFV) unlock the ability for Microsoft to deploy our security capabilities and features at scale across the Open RAN ecosystem, via micro-segmentation and the use of secure containers simultaneously. These characteristics, unique to 5G and enhanced by Microsoft's security maturity, enable a more granular control of sensitive data and workloads than prior generations of networking technology, and enable control in a way that is scalable

[16] *Secure Software Development Framework*, National Institute of Standards and Technology Information Technology Laboratory, available at: https://csrc.nist.gov/projects/ssdf and *Fundamental Practices for Secure Software Development*, Third Edition, SAFECode (Jun. 23, 2020) available at: https://safecode.org/fundamental-practices-secure-software-development-2/

through automation and AI.

B. Cloud Detects and Mitigates Threats Through Security Telemetry and AI

Microsoft processes over 8 trillion daily security signals to assess and protect against sophisticated attacks. We are able to use our massive security signals depth, combined with a global team of experts, our security information and event management (SIEM), and detection and response capabilities paired with AI to protect operator networks, services, and infrastructure. We integrate this security telemetry combined with our cloud security capabilities such as Azure Defender to block malware and server threats, support the broader open source ecosystem through advanced security through platforms like GitHub and provide operators access to the Azure Security Center platform which enables greater visibility into operator security posture and compliance requirements.

C. Cloud Delivers Enhanced 5G Platform Security and Resiliency

When it comes to the dispersed deployment enabled by Open RAN, such as the reliance on data centers and near and far edge compute capabilities, Microsoft is able to address the platform security and resiliency - an important intersection between hardware and software security. We provide multiple capabilities to enhance security and platform integrity in our Azure services for operators. For our cloud infrastructure, we use sophisticated techniques to ensure that the firmware running on that server has not been compromised.[17] Microsoft servers rely on two "roots of trust" to verify the integrity of platform firmware. The first root of trust, called Cerberus, authenticates the integrity of all platform firmware as it is loaded and compares it to the expected value in a platform firmware manifest. If there is a mismatch, the code is not executed, and a remediation process is started to restore to a trusted state. The second root of

[17] Firmware is software installed on the read only memory of a device that provides instructions for the device to communicate with other components.

trust is what we call a Trusted Platform Module (TPM). The TPM is a tamper-resistant, cryptographically secure auditing component with firmware supplied by a trusted third party. Measurements of all components, firmware and configuration settings are recorded during boot in the TPM. The boot measurements are cryptographically signed by the TPM and sent to an Azure Host Attestation Service for validation. Before the platform is granted permission to join the Azure fleet and host customer workloads it must pass validation. If there is a mismatch, the transaction is considered invalid, and the servers are taken offline to bring them back into a compliant or "trusted" state. These capabilities ensure a level of trust is integrated into the firmware which sits a top 5G deployed hardware, and ultimately delivers a level of trust and security to traditional hardware devices that may be deployed in difficult or unsure physical environments.

D. Cloud Leverages Novel Technology Solutions to Secure Supply Chains

The global information and communications technology (ICT) supply chain security is more complex than ever before. The NOI seeks comment on supply chain risk management issues (para. 40). Critical to achieving supply chain security is the ability to protect against persistent and increasingly sophisticated threats against both hardware and software. This requires new and old approaches to strengthen U.S. software and hardware supply chains and enhance the resiliency of IT infrastructure.[18] Fortunately, SDN and NFV represent a shift away from legacy communications and ICT technologies based on hardware, to software-based networks that leverage commercial off-the shelf, or commodity-based hardware. This is rapidly transforming

[18] *See* Microsoft Comments on the U.S. Department of Commerce's Interim Final Rule to implement EO 13873, Securing the Information and Communications Technology and Services Supply Chain, filed Mar. 22, 2021. Available at: https://www.regulations.gov/comment/DOC-2019-0005-0091

the ICT ecosystem, and allows networks to become more flexible and adaptive and leverage cloud security across the networks. SDN can facilitate the incorporation or addition of sophisticated security features in real-time, using AI/ML and advanced cloud security capabilities to rapidly detect and actively mitigate malicious activities. At Microsoft, we also understand how to integrate leading supply chain security risk management practices to enhance the security of cloud services deployed in an Open RAN, such as by leveraging NIST's 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.*[19] Microsoft partners with NIST's National Cybersecurity Center of Excellence to enhance the broader software security supply chain through industry-driven proof-of-concepts in secure development automation technologies and practices to support NIST's goal of accelerating and scaling secure software development technologies.[20]

In addition to the cloud native capabilities which will enhance the security of supply chains, we also encourage the FCC to consider ways to partner across the federal government to continue to incentivize digital solutions in Open RAN to mitigate supply chain risk. For example, software security technologies designed into software packages or code can address security risks by ensuring trust and preventing software from being exploited by bad actors or for malignant uses. These features include: the ability to deploy trusted software updates, including the firmware of compromised devices; automating security policies to, for example, seek out and prevent placement of user or administrator credentials in software code; and, in appropriate cases

[19] Boyens, J., Paulsen, C., Moorthy, R., Bartol, N., *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* NIST SP 800-161 (Apr. 2015) available at: https://csrc.nist.gov/publications/detail/sp/800-161/final

[20]NIST National Cybersecurity Center of Excellence, https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

once in-development standards are finalized, use of software bills of materials (SBOMs) to convey evidence that software consumers can trust the environment in which software was built. Similarly, hardware security technologies built into hardware can further protect against supply chain risks. Solutions include hardware roots-of-trust to verify, protect, or restore system, data, or code integrity; secure co-processors for more robust identity verification; and, in appropriate cases, origin and identity attestation for components in a hardware system. And for more sensitive applications, data security technologies can protect exposure of U.S. data through the supply chain. Features include digital rights management, information flow controls, data tagging and, where appropriate, the use of secure virtual or data lockbox environments.

E. Cloud Engineering Helps Manage and Mature Open Source Security

Open RAN and Open Source software are not one and the same. Open RAN focuses on bringing *open interfaces* to the RAN, while *Open Source software* can be used to implement components sitting behind those Open RAN interfaces.[21] The combination of Open RAN and open source facilitates the effective development of third-party security testing suites and tools, which can lead to a deeper and faster identification of software bugs in the underlying components. Given the questions in the NOI about open source (para 55), we address why open source can be a healthy contributor to an innovative ecosystem that will include both open source and proprietary elements.

Open Source software is an integral component to continued software innovation. According to research published last year[22] by McKinsey & Company, open source adoption was the

[21] The O-RAN Alliance is specifically pursuing both open interfaces and open source, but perhaps open interface efforts are farther along.

[22] Srivastava, S., Trehan,K, Wagle, D. and Wang, J., *Developer Velocity: How software excellence fuels business performance*, McKinsey & Company, (Apr. 2020). Available at:

biggest differentiator for top-performing organizations. Modern software projects are increasingly dependent on Open Source software and components. This can range from whole operating systems to user interfaces, to back-end data analysis, and front-end graphics.

Like most technology and software innovations, Open Source software has led to some amazing benefits, and is also sometimes accompanied by novel security risks that must be understood and managed. For the most part, it is important to understand these risks apply when using any third-party software component, regardless of whether it is open source or closed source software. When it comes to open source security and cloud, Microsoft welcomes the opportunity for the FCC, in collaboration with other government agencies, to seek further public-private partnership opportunities to enhance the open source security ecosystem. We are continuously improving access to, and simplifying use of, security tools and automation on our developer platforms such as GitHub.[23] We are extending security enhancements to tools that we use for our own secure development operations to the broader developer community.[24] Microsoft regularly reviews our security practices and external guidance and do so increasingly with an eye to including more open source security tools and automation strategies.

Open Source software can be used in conjunction with Open RAN, yielding benefits such as additional vendor diversity and improved security. OSS lowers the barrier to entry both for

---

https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/developer-velocity-how-software-excellence-fuels-business-performance

[23] *See* Security, Github, https://github.com/features/security; Github and Azure, Microsoft Azure, https://azure.microsoft.com/en-us/products/github/

[24] For example, we are in the process of strengthening automatic detection capabilities for the CodeQL static analysis tool, which produces analysis artifacts from build servers and is available in GitHub.

consumers of the software, who may be leveraging the software to build new U.S.-based 5G products, and for contributors who wish to improve the software by adding new features, improving performance, or fixing a software defect. Open source fundamentally enables and accelerates research and development and the creation of new technology products, which is why, according to Synopsys' 2020 Open Source Security and Risk Analysis Report,[25] 99% of new codebases include OSS, and OSS made up 70% of the codebases themselves. Put differently, almost all new audited software not only uses open source, but the majority of the software is actually open source components. Mature OSS development practices have been shown to produce more secure software, and that once released, Open Source software's security is often maintained more stringently than non-open source software.[26]

These well-proven benefits and advantages of OSS are why Microsoft is today the world's largest contributor to open source. Microsoft uses OSS extensively in our products and services, and Microsoft's users leverage OSS heavily – especially in the Azure cloud. As Microsoft's Azure for Operators provides a platform that interoperates with Open RAN, we envision a system that will use both open source elements and proprietary elements.

VI. THE FCC, WORKING WITH OTHER DOMESTIC AND INTERNATIONAL AGENCIES, HAS AN IMPORTANT ROLE TO PLAY IN ENABLING NEXT GENERATION WIRELESS NETWORKS, INCLUDING BY SUPPORTING OPEN RAN

As the Commission examines how to support the development of next generation wireless

[25] *Open Source Security and Risk Analysis Report*, Synopsys, 2020. Available at: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2020-ossra-report.pdf

[26] *State of Software Security Report*, Vol 1., Veracode, (Mar. 1, 2010) Available at: https://www.veracode.com/sites/default/files/pdf/resources/reports/state-of-software-security-volume-1-report.pdf

networks, it should consider how the United States and its allies can take a leadership role in 5G and beyond. Leadership in this area will require significant investments, not only in 5G technologies, but also in 6G research, such as the investment made by the European Union. The EU anticipates that 6G networks will take much greater advantage of the cloud.[27] The cloud ecosystem, in turn, unlocks a global developer and partner ecosystem which spurs innovation in the US and allied countries.

As a trusted entity, Microsoft supports the federal government's efforts to lead in next generation wireless networks and will continue its support for future versions of wireless networks and services. The FCC can and should take steps to ensure that the development of Open RAN is supported and not encumbered by government actions. More broadly, the FCC should take steps to support all aspects of next generation wireless networks, including enabling innovation and increased security through cloud native approaches.

In this section, we offer some recommendations for the FCC. Some are directly in the FCC's jurisdiction. Others may require the FCC to coordinate with other U.S. government agencies. Microsoft suggests that the FCC:

- **Use technology neutral policies that promote next generation solutions by enabling the use of cloud, Open RAN, and proprietary and Open Source software.** As network operators move away from RANs provided by a single vendor and to Open RAN networks, combined with cloud, and potentially Open Source software, government agencies should

---

[27] *See* Castro, C. (2021, April 5). EU Has Granted Over €95 Million in Funding for 6G Research. *6GWorld*. https://www.6gworld.com/exclusives/eu-has-granted-over-e95-million-in-funding-for-6g-research/; O'Connor, J., Moore, L., & Cullen, D. (2020, November 4). EU Member States Declare Support for a Next Generation European Cloud Service. *Lexology*. https://www.lexology.com/library/detail.aspx?g=023a5c7f-5b87-4a9a-971a-4581bdd754ec

recognize the variety of potential network configurations and ensure that policies do not inadvertently create disincentives for use of next generation solutions. For example, testbeds should be cloud-friendly. In calling for testbeds, government agencies should not adopt technical requirements that preclude cloud-based products, for example, by requiring that testing be run on specialized hardware.

- **Ensure that reimbursement rules and funding permit OpEx and CapEx funding.** The NOI seeks comment on Commission actions in the context of USF and Rip and Replace (paras 65-70). When the FCC provides funding support or reimbursement for wireless networks, e.g., in the context of universal service support or "rip-and-replace," it should refrain from specifying that monies will be directed only to capital expenditures. It may be more cost-effective and secure, especially for smaller wireless carriers, to use cloud-based products as part of their solutions, and that spending may appear as an operational expenditure.
- **Promote security best practices based on risk-based, internationally harmonized approaches.** The Commission should leverage its convening authority, both domestically and internationally, to facilitate information sharing and best practices for mitigating security threats. Microsoft encourages the FCC and other U.S. agencies to build on existing standards (e.g., NIST), rather than duplicating measures and/or imposing overlapping regulations that could create confusion and unnecessary costs. Where possible, the FCC and other domestic and international agencies should also leverage international security constructs (e.g., the Prague Principles) although unique requirements above those consistent baselines may be appropriate in some circumstances. International harmonization is required to enable a secure, trusted, and diversified 5G supply chain across U.S. and allied countries without

creating fragmented or nationalized markets. Fragmented markets impede the success of American and allied technology providers abroad and undermine efforts to compete with high-risk vendors.

- **Provide incentives for rural carriers to improve security.** The FCC should also consider creating incentives for rural carriers to improve their security, including by taking advantage of the scale enjoyed by the large MNOs, which can be achieved by small carriers through use of cloud-based services. These incentives might be financial, e.g., through the Universal Service Fund or rip-and-replace programs (see NOI at paras. 69-70).
- **Encourage industry to come up with the equivalent of OnGo certification.** An industry certification program for Open RAN can be a significant milestone, where every component provider gets certified. It is extremely important to recognize that setting up this process should not delay or hinder the aggressive momentum seen with Open RAN. As a model, the industry has developed a certification process for devices in the CBRS band known as OnGo certification.[28] The FCC should encourage industry to come up with the equivalent for Open RAN.
- **Support research and development including support for test beds and plugfests to enable innovation.** The NOI seeks comment on testbeds and demonstration projects (paras 62-64). Open RAN is an enabler of innovation in technology in telecom. Government actions, such as providing research grants or funding to create more testbeds and proofs of concept, can speed its adoption.

It is important that the performance of the Open RAN system exceeds or is at par with the

[28] OnGo Certification Program, OnGo Alliance. Available at: https://www.cbrsalliance.org/certification/

proprietary solutions. It is equally important for the ecosystem to have the participation from incumbent vendors and operators as it is to create a broad ecosystem of smaller, newer and innovative companies. As such, test beds and plugfests can bring these parties and researchers together to test and solve issues. For instance, test beds and plugfests can examine the possibility to leverage AI/ML and automation to program the RAN network for the potential to improve spectral efficiency. These research-based groups can address the operations and maintenance of a disaggregated system such as a virtual network. Industry plugfests and test beds create data models and interfaces to enable collection of metrics that can be fed into AI/ML models to gain operational efficiency. Similarly, they can investigate and test zero touch provisioning of systems using automation for the potential to increase the speed of deployment.

In addition to focusing on the supply of 5G infrastructure, government actions, such as providing research grants or funding to create more testbeds and proofs of concept, should incent innovation in the applications that leverage 5G. Potential applications include energy monitoring on the power grid, or more secure and efficient infrastructure in airports and shipping ports. Not only are such applications beneficial in their own right, but they also increase demand for commercially viable 5G networks. Pilot projects should culminate in real world use cases and dual-use commercially available 5G solutions.

- **Partner with and learn from allied countries.** The NOI seeks comment on learning from the experiences of other countries (para 82). Many of the United States' allies are taking steps to enable and deploy Open RAN that can be informative. The FCC and other federal agencies should bring a similar focus to activities that will advance next generation wireless networks, such as the actions undertaken by the United Kingdom and Australia. In the

United Kingdom, for instance, a 5G trials and testbeds program is part of the Government's nationally coordinated program of investment in 5G.[29] The UK program looks to harness areas where the UK believes it has a competitive advantage – such as scientific research, engineering talent and their rich variety of technology businesses. It will explore the benefits and challenges of deploying 5G technologies in order to accelerate the deployment of 5G networks in the UK, maximize the productivity and efficiency benefits to the UK from 5G, and create new opportunities for UK businesses at home and abroad. Supportive regulatory actions, such as the newly created Australian 5G fund, provide another example on how to create such ecosystems. The bulk of the 5G funding will go to establishing the $22.1 million Australian 5G Innovation Initiative.[30] The first round of grants will support 5G trials to rigorously test 5G technology and identify applications and use cases that demonstrate 5G's capabilities and benefits across a range of industry sectors and locations.

One of the policy priorities for the G7 Digital and Technology Track at the June 2021 G7 Meeting will be "telecom diversification." [31] As discussed above, Open RAN will help to enable vendor diversity and a rich ecosystem of developers that operators can use. In addition to the efforts that will be led by the G7, the Quad countries have launched a Critical

[29] *Next Generation Mobile Technologies: An update to the 5G strategy for the UK*, Department for Digital, Culture Media, and Sport (Dec. 2017). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677598/Next_Generation_Mobile_Technologies_An_Update_to_the_5G_Strategy_for_the_UK_Final_Version_with_Citation.pdf#page=7

[30] *Australian 5G Innovation Initiative*, Australian Government (Mar. 31, 2021) Available at: https://business.gov.au/grants-and-programs/australian-5g-innovation-initiative#overview

[31] Digital & Technology Ministers, G7UK 2021, https://www.g7uk.org/digital-technology-ministers/.

and Emerging Technology Working Group to address similar topics.[32]

The FCC should cooperate with like government bodies from these countries and create alliances that will further the work towards secure and open 5G and beyond wireless networks.

- **Build the Workforce.** Open RAN will bring more diversity and innovation to the 5G and next generation wireless networks. For the technology and the new entrants in the market to be successful, the operators, the system integrators, and anyone involved in deploying these networks will need to be trained and qualified. As this is a new technology, it is reasonable to expect that we do not yet have a sufficiently trained workforce, and investment in skilling will be required.

  The FCC should work with industry and with other federal agencies to expand support for STEM education throughout all levels of education and invest in post-secondary education for critical disciplines, such as AI, quantum computing, and cybersecurity.

[32] *Fact Sheet: Quad Summit*, The White House (Mar. 12, 2021) Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/fact-sheet-quad-summit/

VII. CONCLUSION

As the FCC focuses on policies that will enable the buildout of secure and innovative wireless networks, Open RAN will play an important role. The cloud is essential to realizing the full potential of Open RAN. The FCC can support next-generation wireless networks through a focus on Open RAN and cloud, and by taking the specific actions described in these comments.

Respectfully submitted,

/s/ Paula Boyd

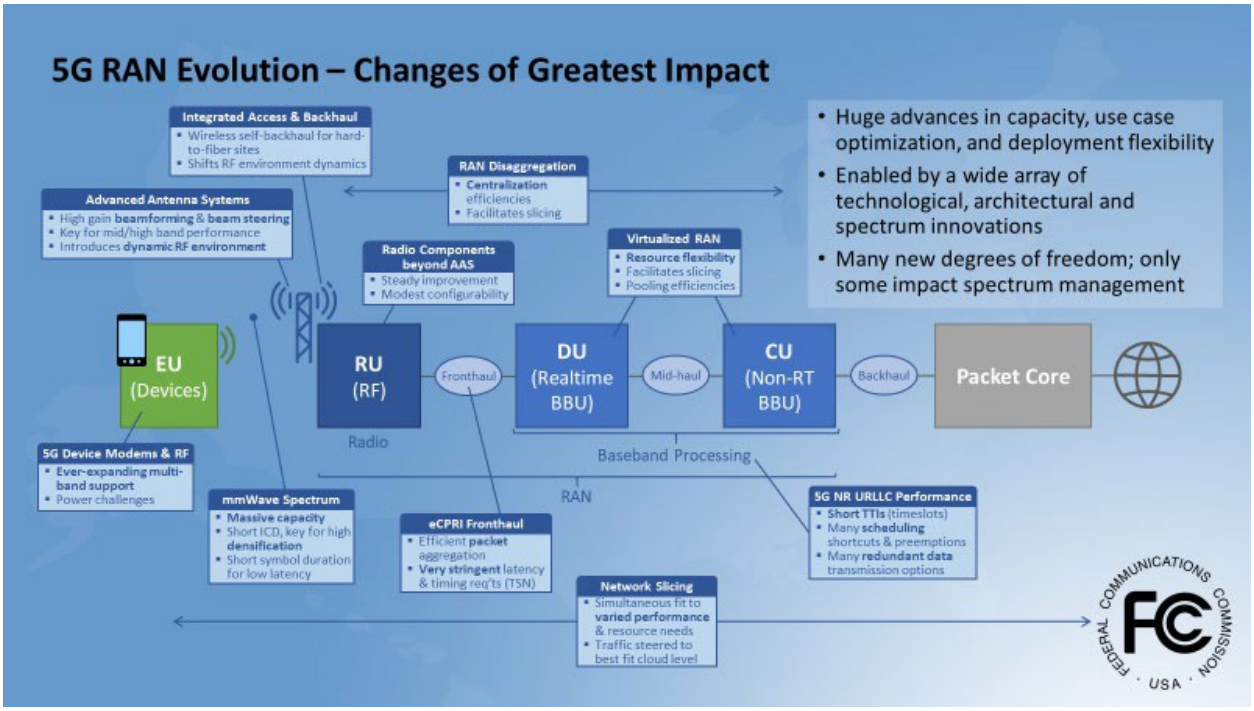
Paula Boyd,
Senior Director, Government Relations and Regulatory Affairs

Stephen Seitz
Principal Corporate Counsel, CELA-PRA

MICROSOFT CORPORATION
901 K Street NW, 11th Floor
Washington, DC 20001
(202) 263-5900

Dated: April 28, 2021

Appendix A



Source, NOI Figure 1. 5G RAN Evolution – Changes of Greatest Impact citing Federal Communications Commission, *Meeting of the Technological Advisory Council (TAC)* (Dec. 1, 2020), https://www.fcc.gov/sites/default/files/tac-presentations-12-1-20.pdf.