Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

January 27, 2023

Submitted via Regulations.gov

Hon. Alan Davidson
Assistant Secretary of Commerce for Communications and Information
NTIA Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave, NW
Washington, DC 20230

Re: Comments of Microsoft Corporation in Response to the Request for Comment on the Public Wireless Supply Chain Innovation Fund Implementation (NTIA-2022-0003)

Dear Administrator Davidson:

Microsoft Corporation (Microsoft) appreciates the opportunity to provide comments in response to the National Telecommunications and Information Administration's (NTIA) request for comments on implementing the Public Wireless Supply Chain Innovation Fund (Innovation Fund).[1]

INTRODUCTION

Over the past few years, there has been an increasingly steady drumbeat for the need to diversify and open the telecommunications supply chain. This has been driven both by security concerns and by the need to improve the negotiating power of operators by introducing new entrants into the market. A key part of this supply chain that can be diversified is the radio access network (RAN), where operators have typically spent most of their investments in network infrastructure.

To address the need for diversification, groups such as the O-RAN Alliance have formed to open up RAN capabilities.[2] In addition, select operator communities from across Europe, the Middle

[1] NTIA, Public Wireless Supply Chain Innovation Fund Implementation, Request for Comment, Docket No. 221202-0260 (Dec. 13, 2022), https://www.federalregister.gov/documents/2022/12/13/2022-26938/public-wireless-supply-chain-innovation-fund-implementation.

[2] O-RAN Alliance, https://www.o-ran.org/ (last visited Jan. 26, 2023).

East, Asia, and Africa have begun experimenting in this space.[3] Governments have also been weighing in, designating telecommunications networks as a national priority and a critical part of infrastructure that needs to be secured and nurtured to drive innovation. An example of this was the UK Government's 5G diversification strategy[4]—a plan to grow the telecommunications supply chain while simultaneously making it more resilient to future trends and threats and enabling more UK based research, innovation and products.

Microsoft's Carrier-Grade Cloud Platform

Microsoft has successfully transformed into an edge and cloud company, so we understand the magnitude of such an evolution. At Microsoft, our guiding principle is to support, develop, and foster a partner-rich ecosystem.[5] We believe that the role that we play best as a cloud provider is to provide a secure, scalable, well-managed carrier-grade platform serving as the enabler for third parties to build upon. [6]

Along with our partners, Microsoft is bringing to life carrier-grade edge-cloud solutions that empower operators globally to deploy Open RAN network functions easily and securely. Our tools and services can manage RAN deployments at scale. With Azure machine learning and AI, a core component of our technologies, operators can perform analytics that optimize performance, improve management, and proactively detect and solve problems.

Security principles designed for the cloud are being adopted to make the platform resilient, to prevent, detect, and respond to threats in the network and across the firmware and

[3] See Stephen Broszio, Major European Operators Commit to Open RAN Deployments, Telekom.com (Jan. 2021), https://www.telekom.com/en/media/media-information/archive/major-european-operators-commit-to-open-ran-deployments-616242; Middle East Operators Collaborate to Support Open RAN, e& (Jul. 2021), https://eand.com/en/news/12-july-2021-middle-east-operators-collaborate-to-support-open-ran.jsp; Ray Le Maistre, Indonesian Operators prep open RAN tests, trials, TelecomTV (Jul. 2020), https://www.telecomtv.com/content/open-networking/indonesian-operators-prep-open-ran-tests-trials-39264/; MTN to launch OpenRAN in Africa, MTN (Jun. 2021), https://www.mtn.com/mtn-to-launch-openran-in-africa/.

[4] 5G Supply Chain Diversification Strategy, Guidance, U.K. Department for Digital Culture, Media & Sport (Dec. 7, 2020), https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy (last visited Jan. 26, 2023).

[5] Yousef Khalidi, Future Proof Your Network with Azure for Operators, Microsoft Azure Blog (Feb. 16, 2021), https://azure.microsoft.com/blog/futureproof-your-network-with-azure-for-operators/.

[6] Azure for Operators, https://azure.microsoft.com/industries/telecommunications/ (last visited Jan. 26, 2023).

telecommunications supply chains.[7] Edge and network monitoring and programmability via open API's will enable a new generation of 5G applications while simultaneously improving operational efficiency. Operators can increase revenues and reduce infrastructure costs while building future-proof solutions.

Microsoft's vision for 5G networks includes the adoption of virtualized RAN (vRAN), as a gradual evolution of the radio access network to Open RAN, from a monolithic approach to virtualization and cloudification of its functional components.

We are aiming to solve some of the challenges of deploying Open and virtualized RAN, such as the management of a multi-vendor environment, ability to scale up and down depending on the needs of our customers, simplifying deployments, and enabling a rich ecosystem of vendors to participate and innovate for better monetization of 5G networks by service providers.

Our short to mid-term approach to vRAN and Open RAN is to build a hybrid cloud platform that provides a common experience across cloud, near and far edge, with cloud automations, zero touch provisioning and life cycle management, and high-performance fabric for real time workloads. Our RAN and platform analytics framework allows service and solution providers to further take advantage of the new architecture and programmable networks and address use cases such as power efficiencies, and anomaly detection in disaggregated systems. It further aims to improve the pace of innovation that can unleash the full potential of programmable and virtualized networks.

The biggest challenge for service providers is also the biggest opportunity for them to support customers' digital transformation and evolution. By promoting a more rapid adoption of Open/Virtual RAN, service providers can take advantage of our collective cloud and network technologies and expertise in areas such as 5G, AI, and IoT to improve the ways in which networks operate.

Summary

In these comments, Microsoft discusses the roles of Open RAN and the cloud and provides recommendations on steps NTIA can take to support the deployment of technologies that will enhance the competitiveness of 5G and success of open, interoperable, standards-based RAN.

First, Open RAN must be paired with cloud capabilities to reach its full potential. As explained below, this will occur in stages, with greater usage of the cloud in later stages. Cloud

[7] Microsoft Security Engineering, https://www.microsoft.com/securityengineering/sdl/resources (last visited Jan. 26, 2023).

technology accelerates security. Open RAN security will depend on cloud security, which is based on international security and risk management standards coupled with unparalleled access to security telemetry and Artificial Intelligence (AI) capabilities to prevent, detect, and respond to old and emerging threats across the network as well as the software and firmware supply chains. Further, cloud technology, includes edge compute, which will enable network operators to scale Open RAN both up and down to match the requirements for public and private networks. Finally, Open RAN deployment will rely on multi-cloud, multi-vendor deployment.

NTIA has an important role to play and can use the Innovation Fund to focus on the following specific areas to foster development of the Open RAN ecosystem and accelerate deployment of Open RAN solutions: closing technology gaps; creating demand for Open RAN solutions; and developing a skilled workforce.

Technology Gaps

As Open RAN solutions continue to develop, NTIA can prioritize projects designed to close certain technology gaps and accelerate the Open RAN deployment timeline. Specifically, Microsoft recommends that NTIA:

- Provide funding to support development of additional components of the ORAN stack – beyond the radio component – that will provide a decisive role in the success of Open RAN deployments, such as:
    - Multi-vendor hybrid platforms, including edge computing;
    - Open RAN Interfaces and Network Elements;
    - Artificial Intelligence; and
    - Security.
- Develop acceptable interoperability criteria. As standards develop slowly, NTIA should encourage the industry along with operators to define an acceptable interoperability criterion, thus assuring a path to adoption.
- Use of open-source software can further enhance aspects such as security.
- Support the creation of an interoperability blueprint and testing facilities that can be accessed by a wide variety of vendors, regardless of size and revenue. This will increase interoperability and vendor diversity.
- Encourage maturity and enhancement of new interfaces defined in O-RAN to address their limitations and accelerate the pace of innovation O-RAN can enable. The open interfaces will allow new entrants in the market and the development of new applications, which in turn will create a rich ecosystem of solutions.

Demand Creation

NTIA can take the following steps to stimulate demand for Open RAN solutions, which will help to accelerate Open RAN deployment and support continued development and investment:

- Promote a more rapid adoption of cloud technologies for Open RAN.
- Provide incentives to move 5G workloads to the cloud, extending to Open RAN.
- Focus on funding initiatives that produce tangible products or services with potential for commercial success and a positive impact on Open RAN competitiveness.
- Create incentives for operators to deploy open solutions that follow open standards through certifiably interoperable implementations.
- Facilitate cooperation between government entities which could benefit the introduction of private 5G networks and co-fund proofs of concept in the specific verticals.
- Include global entities among eligible grant recipients, so long as the direct funding from the grant is targeted at diversifying the global Open RAN ecosystem, including through spending on research, testing, demonstrations, trials, and deployment acceleration in the United States.

Skilled workforce

Finally, NTIA can use the Innovation Fund to assist with building a skilled workforce to help create the next generation of wireless networks as described below.

State of the Industry

1. **What are the chief challenges to the adoption and deployment of open and interoperable, standards-based RAN, such as Open RAN? Are those challenges different for public vs. private networks? What are the challenges for brownfield deployments, in which existing networks are upgraded to incorporate open, interoperable, and standards-based equipment?**

Open RAN adoption and deployment must be considered in the context of 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 and programs that support the emergence and successful evolution of the network.

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. Combining Open RAN with the cloud will enable an ecosystem that is vertically and horizontally diverse, providing network operators with a larger pool of suppliers and more methods to modernize and secure their networks. Furthermore, cloud allows for mobile operators to move away from solution-specific hardware.

Nearly a decade ago, a group of global operators published a whitepaper highlighting the benefits, enablers, and challenges of Network Function Virtualization (NFV) for wireless networks.[8] 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 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 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 move select network functions to the cloud, often starting with those functions that are most easily centralized. Here, leveraging virtualized or containerized network functions in the cloud results in improved security, cost reductions, 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.

An Open RAN ecosystem is a foundational component in evolving next generation networks to fully 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

[8] Network Functions Virtualisation, Network Operator Perspectives on Industry Progress, SDN and OpenFlow World Congress (Oct 2013), https://portal.etsi.org/NFV/NFV_White_Paper2.pdf.

bringing together a diverse ecosystem for a common purpose. RAN components will yield additional benefits, including opportunities for further innovation and enhanced security.

NTIA should focus the Innovation Fund on projects that address some of the main challenges around adoption of Open-RAN, including:

- Centralized management of a large-scale, distributed virtualized network. While most existing testing has focused on interoperability of various RAN elements, additional testing is needed to address automation, security, and power efficiency issues. Lessons learned from greenfield deployments can help with common acceptable criteria and continued innovation to improve power consumption based on new silicon and software/analytics techniques.
- Interoperability between legacy equipment and Open RAN solutions to support brownfield deployments. Further standardization may help to support necessary performance & feature parity between classic RAN and vRAN/O-RAN solutions in brownfield deployments, as well as the seamless interaction necessary to support handovers in brownfield environments.
- Common industry criteria and certification to support interoperability.
- Demand creation for adoption of the new technology.
- The new Open RAN-defined interfaces will need more development. As operators look to include, for instance, a RAN Intelligent Controller (RIC) as an element of the Service Management and Orchestration (SMO) Framework, the new interfaces need to offer flexibility such that new application can be developed at a fast pace that can lower the barriers to entry for new entrants.

The scale of challenges presented in private and public network deployments varies widely. A public network deployment typically requires managing and operating thousands of sites in a disaggregated and multi-vendor environment, necessitating much more automation and AI/Machine Learning (ML) based analytics that can enable operational efficiency and reduce total cost of ownership (TCO). Private networks can benefit from the supply chain diversification that Open RAN enables. Cloud solutions are required for both to play a key role in addressing these challenges and enabling the opportunities with API driven approach that developer ecosystem can leverage.

Microsoft recommends that NTIA fund projects that will further work on covering the technical gaps. Private networks could provide a much easier vehicle for addressing real use cases and creating environments in which innovation can thrive. Implementing the lessons learned from initial private network deployments in large scale operator networks will further the benefits of Open RAN.

NTIA could also work with other government entities to combine funding for private networks in specific verticals, such as agriculture, firefighting, forestry, or defense.

2. **What ongoing public and private sector initiatives may be relevant to the Innovation Fund? What gaps exist from an R&D, commercialization, and standards perspective? How might NTIA best ensure funding is used in a way that complements existing public and private sector initiatives?**

Public and Private Initiatives

A very good example of an existing public-private initiative is the Future Radio Access Network Challenge (FRANC), a UK Department of Digital, Culture, Media, and Sports (DCMS) funded program, which was designed as a follow-on to their diversification strategy.[9] The program identified the need to accelerate Open RAN innovation to meet its target of 35 percent of all network traffic over Open RAN by 2030,[10] as well as spark UK-based innovation in this space.

This initiative accomplishes the dual objectives of growing and diversifying the supply chain as well as supporting a healthy and vibrant Open RAN ecosystem. Microsoft partnered with Intel and Capgemini, industry leaders in Open RAN, and the University of Edinburgh, a leading academic institution, to join us in demonstrating how our ideas could fit together to achieve our mutual objectives. DCMS has endorsed this approach, with the Microsoft-led consortium receiving a Future Radio Access Network Challenge funding award.[11]

The project demonstrated that disaggregated software and hardware are the future of telecommunications networks. This new software-driven programmable network architecture leads to faster rollouts with lower total cost of ownership. Cloud technologies—AI and machine learning analytics, edge computing, large-scale management, self-diagnostics, network programmability, network verification, and global connectivity—can be leveraged to improve

[9] Future RAN: Diversifying the 5G Supply Chain, Guidance, UK Department for Digital Culture, Media & Sport (Aug. 2021), https://www.gov.uk/guidance/future-ran-diversifying-the-5g-supply-chain.

[10] A Joint Statement on the Sunset of 2G and 3G Networks and Public Ambition for Open RAN Rollout as Part of the Telecoms Supply Chain Diversification Strategy, News Story, UK Department for Digital Culture, Media & Sport (Dec. 2021), https://www.gov.uk/government/news/a-joint-statement-on-the-sunsetting-of-2g-and-3g-networks-and-public-ambition-for-open-ran-rollout-as-part-of-the-telecoms-supply-chain-diversificatio.

[11] Future RAN: Diversifying the 5G Supply Chain Competition Winners, Guidance, UK Department for Digital, Culture, Media, & Sport (Oct 2022), https://www.gov.uk/guidance/future-ran-diversifying-the-5g-supply-chain-competition-winners#towards-ai-powered-and-secure-carrier-grade-open-ran-platform.

highly secure operational efficiency of the virtualized RAN. This infrastructure also supports the creation of new revenue streams through the enablement of a developer ecosystem.

NTIA could use a similar approach to provide funding for such initiatives and work with like-minded to share knowledge and opportunities, which can also help spur demand for Open RAN adoption and deployment.

Standards and Open Source

While Open RAN focuses on bringing *open interfaces* to the radio access network, *Open-Source software* (OSS) can be used to implement components sitting behind those Open RAN interfaces. The combination of Open RAN and Open-Source software facilitates 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 about standards, we address why Open-Source software can also be a healthy contributor to an innovative ecosystem that will include both open source and proprietary elements.

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 NTIA, 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. We are extending security enhancements to tools that we use for our own secure development operations to the broader developer community.

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 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, 99% of new codebases include OSS, and OSS made up 70% of the codebases themselves. Put differently, almost all newly audited software uses open-source, and the majority of the software is actually comprised of open-source components.

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 and proprietary elements.

Microsoft recommends that NTIA encourage the use of open-source software to increase innovation, security, and the vendor ecosystem.

3. **What kind of workforce constraints impact the development and deployment of open and interoperable, standards-based RAN, such as Open RAN? How (if at all) can the Innovation Fund help alleviate some of these workforce challenges?**

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 investment in workforce skilling to ensure sufficiently trained will be required.

Microsoft recommends that NTIA 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 radio, virtualization/cloudification, AI, and cybersecurity.

The existing workforce will need to develop new skillset such as virtualization, cloud tools, security, to name just a few, to manage these Open-RAN networks. Incentivizing operators and organizations to upskill their existing workforce to gain these new skillsets will enable this technology to be adopted in commercial networks faster.

4. **What is the current climate for private investment in Open RAN, and how can the Innovation Fund help increase and accelerate the pace of investment by public and private entities?**

Microsoft concurs with the observations made by ORPC that the process of funding projects through a combination of private and public entities should not necessitate any form of in-kind contributions from vendors.

Establishing an innovation fund can serve as a catalyst for developing new products and pave the way for their commercialization. In turn, this will foster greater private investment as these newly developed products begin to generate revenue.

5. **How do global supply chains impact the open, interoperable, and standards-based RAN market, particularly in terms of procuring equipment for trials or deployments?**

A global supply chain benefits all parties, customers, operators, vendors, and governments. For operators, it provides flexibility in purchase decisions, avoids vendor lock-in, and enables them to offer more value-added services to their customers. For vendors, it enables a broader market segment that they can address with the same technology to leverage economies of scale. And for governments, it can enhance security and enable many new locally-based solutions, thus contributing to GDP.

Technology Development and Standards

6. **What open and interoperable, standards-based network elements, including RAN and core network elements, would most benefit from additional research and development (R&D) supported by the Innovation Fund?**

Microsoft encourages NTIA to look at all components of the Open RAN stack needing further investments. These components include the Radio unit, the RAN software stack of virtual Central Unit (vCU) and virtual Distributed Unit (vDU), the Hybrid-cloud platform, AI/ML, and enhanced Open-RAN interfaces and network elements, which are all necessary components that will play a decisive role in the success of the Open RAN deployments.

Hybrid Cloud Platform

Hybrid cloud platform refers to the virtualized platform solution that provides a single management interface and a common software platform to deploy highly distributed workloads from edge to central cloud, thus lowering costs for large scale deployments.

A common example of a hybrid cloud is combining a public cloud environment with an on-premises environment (in this case, servers deployed and owned by a mobile operator). Combining these two or more environments with a single management interface and common software platform enables simpler management and lower cost while still being able to meet the strict performance requirements of running a virtualized Open RAN.

Virtual RAN and Open RAN edge computing workloads can significantly benefit from a hybrid cloud platform solution.

Edge computing, which is needed for massive scale Open RAN deployments, is an important component of next generation wireless networks. Edge computing is the movement of bringing 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. RAN is one such latency sensitive application and is envisioned to be deployed in a hybrid cloud fashion.

As more aspects of the RAN become virtual, the telco 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-efficient algorithms of cloud platforms and improve failover scenarios across servers. Because the RAN functions are disaggregated, 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.

Such a scalable multi-vendor hybrid cloud platform warrants increased automation and management solutions driven by AI/ML.

Microsoft has invested many intellectual and engineering cycles in the development of the Azure public cloud: a sophisticated, robust framework that manages millions of servers and several hundred thousand network elements distributed in over 140 countries around the world. We have built tools and expertise to maintain these systems, use AI to predict problem areas and solve them before they become issues, and provide transparency in the performance and efficiency of a very large and complicated system.

At Microsoft, we believe these tools and expertise are needed to manage and optimize the telecommunication infrastructure. This is because the evolving infrastructure for telecommunications operators includes elements of edge and cloud computing that lend themselves well to global management.

For the ecosystem, a unified framework delivers the freedom to use the tools they are familiar with while focusing more on the business logic in their applications.

O-RAN Interfaces and Network Elements

The new interfaces introduced in Open RAN are in the early stages of standardization and can be enhanced, including the interfaces to manage the O-Cloud and RIC. O-Cloud is a cloud-computing platform made up of a collection of physical infrastructure nodes for hosting Open RAN, including: network functions such as Near-Real Time RAN Intelligent Controller (RIC), O-RAN Central Unit-Control Plane (O-CU-CP), O-RAN Central Unit-User Plane (O-CU-UP), and O-RAN Distributed Unit (O-DU); software components such as the operating System, virtual machine monitor, and container runtime; and service management and orchestration functions. Furthermore, the current RIC architecture envisions uses cases with a latency of >10ms. However, there are use cases such as real-time power management which would need to work with latency of<10ms.[12]

Inter-operation of legacy RAN with Open RAN solutions will be an important focus for brownfield deployments, and interfaces may require standardization to enable this seamless co-existence of solutions.

Artificial Intelligence

The benefits of Artificial Intelligence and Machine Learning (AI/ML) will prove to be significant from several perspectives, such as:

- Optimizing current infrastructure assets to deliver a more effective service;
- Planning service roll outs to ensure that the right infrastructure is deployed for the current and future levels of demand;
- Leveraging the power of big customer data to deliver improved service levels;
- Reducing service failures and contingency planning in case of service outages;
- Automated compensation for cell outage**,** drawing from surrounding cells to return lost coverage. This is of great use in daily situations and has also been proven during extreme situations, such as natural disasters;
- Channel Modeling, Prediction and Propagation;
- Dynamic Spectrum Sharing;
- Quality of Service Optimization and Traffic Classification;
- Optimizing WAN connectivity between Edge sites and the Public Cloud;

[12] See Yousef Khalidi, Microsoft Innovation in RAN Analytics and Control, Microsoft Azure Blog (Dec. 21, 2022), https://azure.microsoft.com/en-us/blog/microsoft-innovation-in-ran-analytics-and-control/.

- Security Optimization and Threat Detection;
- Fraud Detection and Prevention; and
- Sustainability.

Artificial Intelligence solutions can be delivered through the cloud to enable Communications Service Providers (CSPs) to automate network operations and service assurance, cutting costs, increasing, agility and boosting subscriber experience.

Integration of AI/ML into Open RAN deployments should be strongly encouraged for large scale networks. NTIA should also encourage smaller service providers to adopt Artificial Intelligence as a Service.

Security is addressed in the responses to questions 17 to 20 below.

7. **Are the 5G and open and interoperable RAN standards environments sufficiently mature to produce stable, interoperable, cost effective, and market-ready RAN products? If not: What barriers are faced in the standards environment for open and interoperable RAN? What is required, from a standards perspective, to improve stability, interoperability, cost effectiveness, and market readiness? What criteria should be used to define equipment as compliant with open standards for multivendor network equipment interoperability?**

One of the biggest barriers to entry is the complexity of standards and compliance requirements. NTIA could help by funding the creation of a normalized list of these requirements, which could cover all the standards and eliminate the complexity involved.

Furthermore, numerous standards related to the Open RAN platform layers (such as O-Cloud) are still in an immature state, representing a significant obstacle for the rapid adoption of Open RAN technology. NTIA could play a crucial role in addressing this issue by deploying testbeds to increase the understanding and practical experience of real-world requirements. These testbeds could be utilized to develop solutions that would ultimately lead to a more efficient standardization process, akin to what has been observed in the Information Technology industry over the past several decades.

Integration, Interoperability, and Certification

9. **How can projects funded through the Innovation Fund most effectively support promoting and deploying compatibility of new 5G equipment with future open, interoperable, and standards-based equipment? Are interoperability testing and debugging events (e.g., "plugfests") an effective mechanism to support this goal? Are there other models that work better?**

NTIA should support enabling a common set of industry-wide acceptable criteria of inter-operability of network elements with each other and with cloud platform. NTIA should further incentivize the commercial adoption of such solutions. Working with friendly governments, NTIA can further impact the global presence and demand generation.

10. **How can projects funded through the program most effectively support the "integration of multi-vendor network environments"?**

Enabling the setup of comprehensive Open Testing and Integration Centres (OTIC) labs with the common certification criteria. Additionally, there should be projects that focus on areas beyond inter-op, like cloud management, Power efficiency, security, and AI/ML. This should include inter-operability of Classic RAN and Open RAN solutions.

11. **How do certification programs impact commercial adoption and deployment? Is certification of open, interoperable, standards-based equipment necessary for a successful marketplace? What bodies or for a would be appropriate to host such a certification process?**

Support research and development, including support for test beds and plugfests to enable innovation.

Open RAN is an enabler of innovation in telecom technology. Government actions, such as 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 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.

NTIA should provide funding to create more testbeds and proofs of concept, which should incent innovation in the applications that leverage 5G. Pilot projects should culminate in real world use cases and dual-use commercially available 5G solutions.

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.

Certification enables an industry wide acceptable criterion for commercial adoption and limits the need for every operator to do their own verification. It is necessary as it will provide the vendor community with a clear and easier path into operator networks. It enables operators to accept new solutions with lesser self-validation/testing and higher confidence. However, we highly recommend that such certification should focus on the most important aspects only, for example, inter-operability between Open RAN network elements. The certification should also rely on existing best practices. This will enable faster time to market.

NTIA should encourage industry to come up with the equivalent for Open RAN.

12. **What existing gaps or barriers are presented in the current RAN and open and interoperable, standards-based RAN certification regimes? Are there alternative processes to certification that may prove more agile, economical, or effective than certification? What role, if any, should NTIA take in addressing gaps and barriers in open and interoperable, standards-based RAN certification regimes?**

The report on NSC study of Open RAN research and testing facilities represents an accurate view of today’s environment. NTIA should support further focus on cloud platform, automation, power efficiency and AI/ML.

NTIA could also play the role of facilitator and help to create market demand and incentives for the ecosystem to work together. We believe the decision to adopt technology should still be left with the operators and not mandated.

Trials, Pilots, Use Cases, and Market Development

13. What are the foreseeable use cases for open and interoperable, standards based networks, such as Open RAN, including for public and private 5G networks? What kinds of use cases, if any, should be prioritized?

Open RAN benefits apply to both public and private networks. For Public networks, the most important use case continues to be consumer cellular networks. As noted before, the challenges for macro networks is different from private networks in terms of scale, but there are a lot of commonalities that exist. For example, cloud environment, platform automation, AI/ML, and security.

While the private LTE/5G network market is still in its infancy, enterprise spending is projected to reach $7.7 billion globally by 2027 and to grow at a CAGR of 48% between 2021-2027.[13] The manufacturing industry will be the biggest sector in terms of enterprise spending (circa 40% of total) followed by mining, oil and gas (31%) and logistics and tracking (17%). Compute spending attached to enterprise 5G software development is growing at a CAGR of 99% driven by investments concentrated in the automotive, public sector, healthcare and manufacturing.

Other potential use cases, in addition the ones stated at the front of the document (agriculture, firefighting, forestry, DoD) could also 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.

14. What kinds of trials, use cases, feasibility studies, or proofs of concept will help achieve the goals identified in 47 U.S.C. 906(a)(1)(C), including accelerating commercial deployments? What kinds of testbeds, trials, and pilots, if any, should be prioritized?

These efforts can be split into two priority categories:

1. Basic inter-operability of virtual or Open RAN network elements. This work should include validation of fronthaul, vCU-vDU interfaces, etc, as well as inter-operability with legacy/classic RAN and deployment validation of vRAN network functions on the cloud

[13] Ibraheem Kasujee, Spending on Private Networks Will Reach USD7.7 Billion in 2027, but Challenges to Adoption Persist, Analysys Mason (Oct. 2022), https://www.analysysmason.com/research/content/articles/private-networks-forecast-rma17/.

platform. As explained above, there should be a common set of validation criteria, and there should be enough room for each vendor to provide their own value proposition on top of this standard inter-operability.

2. Solutions that further enhance Open RAN potential. This work should include an increased focus on solutions for RAN and platform analytics, power efficiency, AI/ML use cases, and security detection. Enabling the use of current cloud best practices from cloud adopting them into Open RAN with minimal changes.

16. What sort of outcomes would be required from proof-of-concept pilots and trials to enable widespread adoption and deployment of open and interoperable, standards-based RAN, such as Open RAN?

A strong Tier 1 operator presence is needed in these proof-of-concept pilots and trials. The pilots and trials should be aimed at understanding potential gaps and solutions, which will not be possible without a strong operator presence. A successful proof of concept should mature from technology readiness to product readiness and deployments.

Security: Questions 17 to 20

17. "Promoting and deploying security features enhancing the integrity and availability of equipment in multi-vendor networks," is a key aim of the Innovation Fund (47 U.S.C 906(a)(1)(C)(vi)). How can the projects and initiatives funded through the program best address this goal and alleviate some of the ongoing concerns relating to the security of open and interoperable, standards-based RAN? What role should security reporting play in the program's criteria? What role should security elements or requirements, such as industry standards, best practices, and frameworks, play in the program's criteria?

18. What steps are companies already taking to address security concerns?

19. What role can the Innovation Fund play in strengthening the security of open and interoperable, standards-based RAN?

20. How is the "zero-trust model" currently applied to 5G network deployment, for both traditional and open and interoperable, standards-based RAN? What work remains in this space?

The communication sector is undergoing rapid digital transformation. More than ever, operators and vendors are seeking to deploy high-quality, cost-minded networks without sacrificing security and resilience to protect critical infrastructure. Meanwhile, nation state groups' targeting of critical infrastructure increased in the past year, with actors' focusing on companies in the IT sector, financial services, transportation systems, and communications infrastructure. Today's communication networks need to adapt architectures based on new security principles and capabilities, involving a model of shared responsibility. There is also a need to make the network more resilient to failures beyond cyberattacks as natural disasters – related to the climate crisis (e.g., floods, fires) and energy- threaten greater disruption.

NTIA can enhance the security and resiliency of multi-vendor networks by encouraging operators and vendors to 1.) incorporate cloud security across multi-vendor networks; 2.) deploy zero trust security principles across networks; 3.) leverage NTIA and NIST's existing Software Bill of Materials (SBOM) policies and guidance; and finally, 4.) provide a clear, consistent reporting obligations.

1. *Incorporate cloud security across multi-vendor networks.*

Cloud computing is a seismic shift from traditional computing, enabling users to do more with greater speed and agility. In part, this shift is due to the way in which cloud services are provisioned and maintained, allowing customers to tap into the power of cloud computing datacenters and services without having to build, manage, or maintain them. Cloud is uniquely positioned to provide elevated security across a multi-vendor communication network. Cloud already provides a secure platform across all critical infrastructure sectors from banking, energy, agriculture, to healthcare, and government services.

Cloud can enhance multi-vendor network security by delivering:

- A better understanding of and more proactive response to the unique threat environment telecommunication networks face. Especially for hyperscale cloud providers, a large pool of clients and managed infrastructure means a wider security intelligence view, more frequent and accurate threat identification, and more proactive mitigating action. For instance, Microsoft quarantines and examines email attachments blocked by our advanced threat protection service, and if malware is found, then we proactively protect all our customers from similar threats.[14]

- Security as a core business function. Microsoft recognizes that trust is a fundamental part of our business model, and we do our utmost to earn it. Cloud service providers also use

[14] Increase Threat Protection for Microsoft 365 for Business, Microsoft Learn (Dec. 12, 2022), https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/increase-threat-protection?view=o365-worldwide.

security as a differentiator, hiring the best talent and investing significant resources. Microsoft invests more than $4 billion in security annually. [15]

- Improved security and operational resiliency by incorporating security as a function of greater awareness. For example, in continuing to rely on legacy hardware and IT, many telecommunications organizations lack awareness of their overall cyber risk exposure. The process of migrating data, services, and operational technology (OT) to a cloud environment can act as a forcing function for cyber risk assessments and governance efforts. Cloud migration especially enhances data governance, helping organizations increase awareness of what data they retain and how they treat it.

2. *Deploy zero trust security principles across vendor networks.*

Cyberattacks are a threat to both national and economic security requiring communication networks to take steps to strengthen operational security. While a range of near- and longer-term activities are ultimately needed to foster ecosystem-wide shifts in cybersecurity risk management, data also indicates that improving basic cyber hygiene practices can have significant impact on risk posture. A few zero trust cyber hygiene practices protect against most attacks. These include enabling Multi Factor Authentication (MFA), a process in which users are prompted during the sign-in process for an additional form of authentication, such as a code sent to their mobile phone, email, or other application or a fingerprint scan.[16] Applying Least Privilege Access, which requires restricting access to resources to only those that require it for specific jobs, rather than granting broad access to any verified user. In a Zero Trust model, every access request is fully authenticated (via MFA), authorized (via least privilege access), and encrypted before access is granted.

3. *Leverage NTIA and NIST existing SBOM security policies and guidance.*

Microsoft continues to invest in supply chain security[17], and Executive Order 14028 (“Improving the Nation’s Cybersecurity”) underlines the importance of these investments and has been a

[15] Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation’s Cybersecurity, Fact Sheet, The White House (Aug. 25, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

[16] Implementing a Zero Trust Security Model at Microsoft, Microsoft Inside Track (Jan. 10, 2023), https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/.

[17] Bret Arsenault, Continued Investments in Supply Chain Security in Support of the Cybersecurity Executive Order, Microsoft Public Sector Blog (May 10, 2022),

catalyst for our current initiatives. These initiatives focus on enhancing supply chain transparency, evolving secure software development and operational security, and helping customers modernize their IT infrastructure. Open collaboration is essential to supply chain security and we're committed to partnering with the public and private sectors on these initiatives. We believe that NTIA should consider how it could incorporate the current NIST Guidance for industry best practices across communication networks supply chain security.

4. *Provide a clear, consistent reporting obligation for communication network vendors.*

Microsoft supports a clear, consistent obligation for private sector organizations to disclose when they're impacted by a significant cyber incident confirmed by their incident response teams. With even more sophisticated and well-resourced nation state cyberattacks on the horizon, greater transparency and increased cybersecurity incident information sharing between governments and the security community are essential components of any strategy to enable us to prevent and respond to those attacks.

The primary focus of incident reporting regimes should be on facilitating a faster, better coordinated, and more effective response in support of organizations impacted by an attack and/or acting as ecosystem-wide responders. Data can also be leveraged to improve understanding of risk and effective mitigation and response activities over time. For situational awareness of potential threats or risks, we encourage NTIA to leverage complementary efforts rather than mandatory incident reporting regimes.

Program Execution and Monitoring

21. Transparency and accountability are critical to programs such as the Innovation Fund. What kind of metrics and data should NTIA collect from awardees to evaluate the impact of the projects being funded?

There are several key metrics and data points that NTIA should collect from awardees to evaluate the impact of projects being funded through the Innovation Fund, including:

- Project duration: NTIA should collect data on the duration required to construct a proof of concept and the extent to which the implementation can be used in practical settings.
- Project scale: The funded projects should specify the scale of implementation.
- Project outcomes: NTIA should collect data on the specific outcomes and objectives of each project, such as the amount of funding leveraged.

https://techcommunity.microsoft.com/t5/public-sector-blog/continued-investments-in-supply-chain-security-in-support-of-the/ba-p/3348709.

- Public benefit: NTIA should collect data on the benefit of each project, such as industries best served by the project.
- Return on Investment: NTIA should measure the return on investment of each project, such as the ratio of the project's benefits to its costs.
- Collaboration and Partnerships: NTIA should track the collaboration and partnerships formed as a result of each project, such as the number of other organizations or companies that were involved in the project.
- Follow-up: NTIA should track the long-term effects and sustainability of the projects, to see if the project has continued to bring benefits even after the funding has ended.

These metrics will provide valuable insight into the effectiveness and impact of the projects being funded. These results can serve as a benchmark for progress and aid in identifying areas for improvement.

The awardees should provide timely and ongoing reports on the work being done, and results should be published and available to see and learn from.

NTIA could further help with knowledge dissemination in various industry forums and within the NTIA sponsored sessions and projects.

22. How can NTIA ensure that a diverse array of stakeholders can compete for funding through the program? Are there any types of stakeholders NTIA should ensure are represented?

Setting up multiple projects with a diverse focus and encouraging a consortium to be formed for the awardees will be the most effective way to encourage collaboration. Stakeholders should include cloud providers, virtual and Open RAN network function providers, Open-RU providers, operators, testing solution providers, Silicon and COTS solution providers, system integrators, O-RAN Network element providers like RIC, SMO, and last but not least, the developer/startup companies that provide SW solutions using analytics and AI/ML.

23. How (if at all) should NTIA promote teaming and/or encourage industry consortiums to apply for grants?

The formation of consortia to provide project proposals could be a beneficial way to encourage collaboration. NTIA can further help the creation of such consortiums by setting up several fast-pitch sessions for different projects.

25. How can the fund ensure that programs promote U.S. competitiveness in the 5G market? Should NTIA require that grantee projects take place in the U.S.? How should NTIA address potential grantees based in the U.S. with significant overseas operations and potential grantees not based in the U.S. (i.e., parent companies headquartered overseas) with significant U.S.-based operations? What requirements, if any, should NTIA take to ensure "American-made" network components are used? What criteria (if any) should be used to consider whether a component is "American-made"?

Microsoft agrees with ORPC that global entities should be eligible for grants so long as the direct funding from the grant is targeted at diversifying the global Open RAN ecosystem, including through spending on research, testing, demonstrations, trials, and deployment acceleration in the United States.

We also agree that as NTIA drafts the Wireless Innovation Fund Notice of Funding Opportunity, it should:

1. Prioritize projects that will broadly benefit the competitive open RAN ecosystem;
2. Encourage the findings/product/results of Innovation Fund-supported projects to be made widely available;
3. Recognize the global nature of this effort by encouraging engagement from international organizations and allowing allied/partner-headquartered entities to compete for funding;
4. Consider the complementarity of projects (i.e., opportunities for multiple projects to augment each other); and
5. Consider the full range of activities needed to spur innovation and deployment (including R&D, lab coordination/certification, workforce development, international coordination, etc.).

26. How, if at all, should NTIA collaborate with like-minded governments to achieve Innovation Fund goals?

To meet these goals will require not only U.S. engagement as contemplated by this RFC, but also engagement by allied nations working together to build a supply chain coalition that will be able to withstand geopolitical disruptions and ensure continuity and security in the face of future disruptions.

Enhanced multilateral cooperation on supply chain resiliency and security efforts in a way that's consistent with global partnerships is also critical to address these challenges. Initiatives proposed by the European Commission under the umbrella of the European Chips Act, the U.S.-EU Trade and Technology Council, and the evolving Indo-Pacific Trade strategy, each represent a unique opportunity to strengthen and diversify supply chains and to build complementary and diverse manufacturing and research capabilities across allied-nations.

Conclusion

We appreciate the opportunity to provide comments to NTIA regarding the Wireless Innovation Fund. Open RAN will play an important role in enabling the buildout of secure and innovative wireless networks. The cloud is essential to realizing the full potential of Open RAN. The NTIA can support next-generation wireless networks through a focus on Open RAN and cloud, and by taking the specific actions described in these comments. If you have additional questions, please reach out via email at robertblair@microsoft.com or phone at (202) 263-5900.