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

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

COMMENTS OF DISH NETWORK CORPORATION

DISH Network Corporation ("DISH") respectfully responds to the Federal Communications Commission's ("Commission") Notice of Inquiry ("NOI") seeking comment on the opportunities and challenges presented by open and virtualized radio access networks.[1] DISH supports the Commission's efforts to explore the benefits of this new architecture and encourages it to adopt targeted proposals that will help spur Open RAN adoption among American carriers.[2] Given the significant benefits Open RAN can provide to U.S. telecommunication supply chains, DISH believes the Commission should, among other things, support robust funding of Open RAN grants to bring the ecosystem to scale and provide carriers working to "Rip-and-Replace" currently installed equipment and services more time to adopt and deploy Open RAN solutions.

I. INTRODUCTION

DISH is a connectivity company that has served as a disruptive force in the pay-TV market since 1980. Building on its record of innovation, in 2020, DISH entered the retail wireless business through its acquisition of the Boost Mobile and Ting Mobile brands and customer assets. DISH has also

[1] *Promoting the Deployment of 5G Open Radio Access Networks*, Notice of Inquiry, FCC 21-63 (rel. Feb 24, 2021) ("NOI").

[2] As used herein, the term "Open RAN" refers to networks that are compliant with O-RAN Alliance specifications. *See* https://www.o-ran.org/specifications.

invested more than $22 billion in wireless spectrum assets over the past decade, with the goal of disrupting the wireless industry. DISH is building the nation's first cloud-native, Open RAN-based 5G broadband network, with Las Vegas as our first city later this year.[3]

DISH's emergence as a wireless competitor means that it will be a critical participant in the United States' race to 5G. Among other developments, DISH has entered into multi-year agreements with over 20 partners providing Open RAN-based solutions, including Mavenir, Altiostar, Amazon, VMWare, Nokia, Fujitsu, MTI, Intel, Qualcomm, Palo Alto Networks, MATRIXX, DigitalRoute, Amdocs, Netcracker Technology, Aviat and Blue Planet, a majority of which are U.S.-based companies.

In December 2020, DISH reached a significant milestone by completing its first fully Open RAN-compliant network communication. In doing so, DISH validated end-to-end 5G connections using the industry's first Open RAN compliant FCC radio, developed by MTI, alongside software partner Mavenir and core vendor Nokia. As a result, DISH brings a unique perspective to this proceeding, as it has experienced the benefits of Open RAN technologies first-hand.

II. OPEN RAN OFFERS UNIQUE ADVANTAGES THAT WILL SPUR AMERICAN COMPETITIVENESS

A. Open RAN Networks Increase Vendor Diversity

Today, legacy RAN networks are closed ecosystems that utilize proprietary interfaces with radio units and baseband units at every cell tower, with no U.S.-based suppliers. Open RAN will provide significant public interest benefits, including injecting competition into the RAN ecosystem and unlocking the full economic benefits of 5G. The Open RAN model allows multiple vendors to coexist and compete within a single network. Open RAN will liberate wireless operators from reliance on a

[3] DISH, "*DISH and AWS Form Strategic Collaboration to Reinvent 5G Connectivity and Innovation*" (April 21, 2021), https://dish.gcs-web.com/news-releases/news-release-details/dish-and-aws-form-strategic-collaboration-reinvent-5g.

single vendor for all components of their network architecture. This, in turn, will enhance our nation's security by eliminating the single point of failure that exists in legacy networks today.

B. Open RAN Will Enhance Spectrum Utilization and Enable Network Slicing

By utilizing an Open RAN model, with standardized, open and interoperable interfaces between the Radio Unit (RU), Central Unit (CU) and Distributed Units (DU), operators can enable a more rapid deployment of new spectrum. Through advances in radio and antenna technologies, as well as disaggregated hardware and software, radios are able to carry multiple spectrum bands. This allows 5G infrastructure to be leveraged and additional spectrum to be deployed and integrated into the 5G core network.

Further, by bringing together innovations such as the distributed cloud, edge computing, and network slicing, a software-based network can provide enterprise users with a customizable, secure network solution. Enterprise customers can manage and control their slice of the network and allocated spectrum as if it were privately operated. Moreover, the network slices are not static and can be dynamically updated based on the needs and requirements of the customer. All of these benefits will enhance spectrum utility.

III. OPEN RAN WILL ENHANCE NATIONAL SECURITY

There is a bipartisan consensus among national security and economic leaders in Congress that the transition to Open RAN is vital to core U.S. national interests, as well as the interests of allied nations. The ability to mix-and-match with different suppliers providing different components of the network can increase competition and prevent the "lock-in" effect where proprietary or semi-proprietary implementations of RAN components inhibit competition among suppliers. By embracing an Open

RAN model, operators can eliminate their reliance on a single foreign-owned RAN provider - *i.e.* the single point of failure problem.

As President Biden stated in his February 24 Executive Order on America's supply chains, "close cooperation on resilient supply chains with partners who share our values will foster collective economic and national security and strengthen the capacity to respond to international disasters and emergencies."[4] U.S. policy therefore should expressly aim to nurture a diverse, competitive collection of suppliers based in the United States and at other allied countries.

IV. DISH'S OPEN RAN FRAMEWORK DEMONSTRATES THE BENEFITS OF THIS INNOVATIVE ARCHITECTURE

In today's software-driven world, secure connectivity is essential, enabling businesses to increase productivity, transform the way they operate and generate a higher return on investment. 5G connectivity supports new business models and delivers cutting-edge services and products. In contrast, traditional wireless networks are challenged to adequately meet customers' future security requirements and expectations. This is because traditional wireless networks are built upon vertically integrated, proprietary systems, which are based on closed-network security models.

To meet customers' needs, DISH sought to design and build an alternative, next-generation network and system architecture that offers state-of-the-art technology and security. As a result, DISH developed a cloud-native solution that integrates network security from the foundation up. To support this effort, DISH selected strategic partners that provide best-in-class security solutions, giving much of the control back to the customer. With these key strategic partners, DISH will offer customers unprecedented visibility, application programming interfaces (APIs), tools and security capabilities to complement their existing security model. With these features, DISH's network security will be more

[4] Executive Order on America's Supply Chains (Feb. 24, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

controllable, agile and scalable than traditional networks. By adopting an Open RAN model, DISH's network will have significant benefits over traditional vertical networks, including security, network slicing and services orchestration, and the integration of multiple Open RAN vendors.

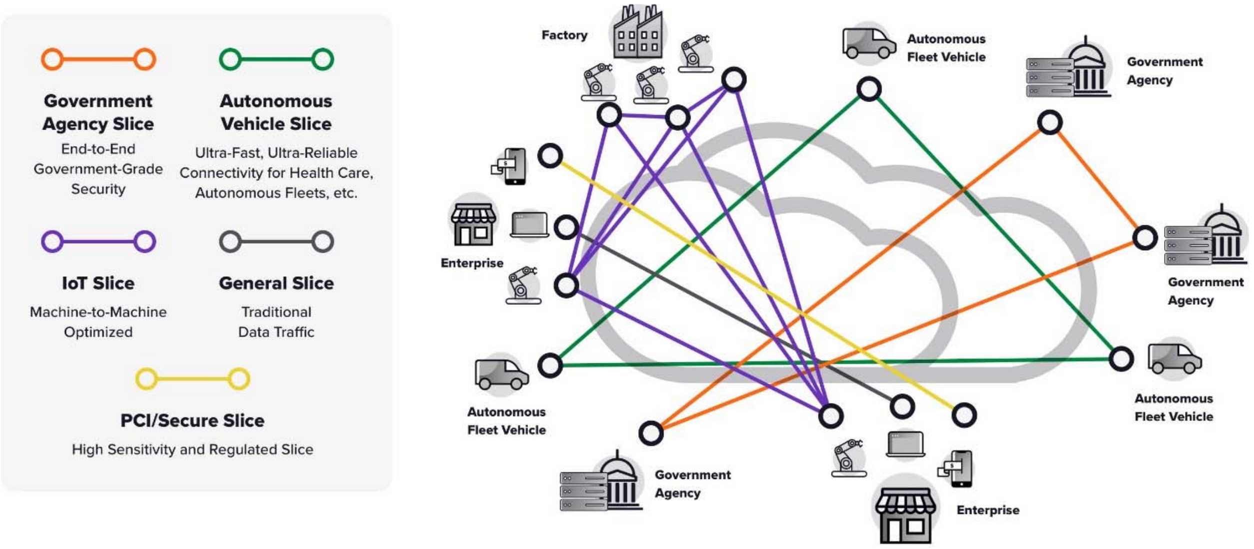
Zero-Trust Model. DISH is adopting a "secure by design" strategy based on a zero-trust model. This model incorporates certification and key management with advanced, multifactor client authentication, allowing DISH to integrate best practices into its products while embracing security design principles. With this construct in place, DISH's network can rapidly respond to the ever-changing security needs of enterprise customers. DISH will continuously iterate, modify and enhance its network at the speed of its customers. As part of the zero-trust model, DISH is taking the "never trust, always verify" approach. Zero-trust provides threat prevention and more control for both DISH's internal operations and its network customers.

Customer Empowerment through Network Slicing and Service Orchestration. DISH will offer innovative ways to empower customers on the network. Using the most advanced security solutions, DISH's network will be free from the limitations of traditional technology and will give customers more control with access to on-demand, secure network slices, encrypted connections, and secure, immersive experiences. A key enabler of this level of control is support for 5G secure slicing, providing customers with their own private 5G network.

5G network slicing in a cloud-native, Open RAN environment enables virtualized, logical networks to be interleaved on top of a common physical infrastructure, essentially functioning as a next-generation virtual private network (VPN). Each network slice is provisioned logically as a separate end-to-end network, tailored to meet the unique requirements and service level agreements (SLAs) for each customer application. This network slicing leverages software-defined networking and the virtualization of 5G core network functions.

As shown in Figure 1 below, DISH will use network slicing to offer end-to-end network services, delivering applications customized to the end-user. New verticals requiring massive connectivity, immersive experiences like virtual reality/augmented reality (VR/AR), machine-to-machine automation and more will be made possible with DISH's network, enabling higher performance, improved predictability, lower cost and greater control over the customer experience.

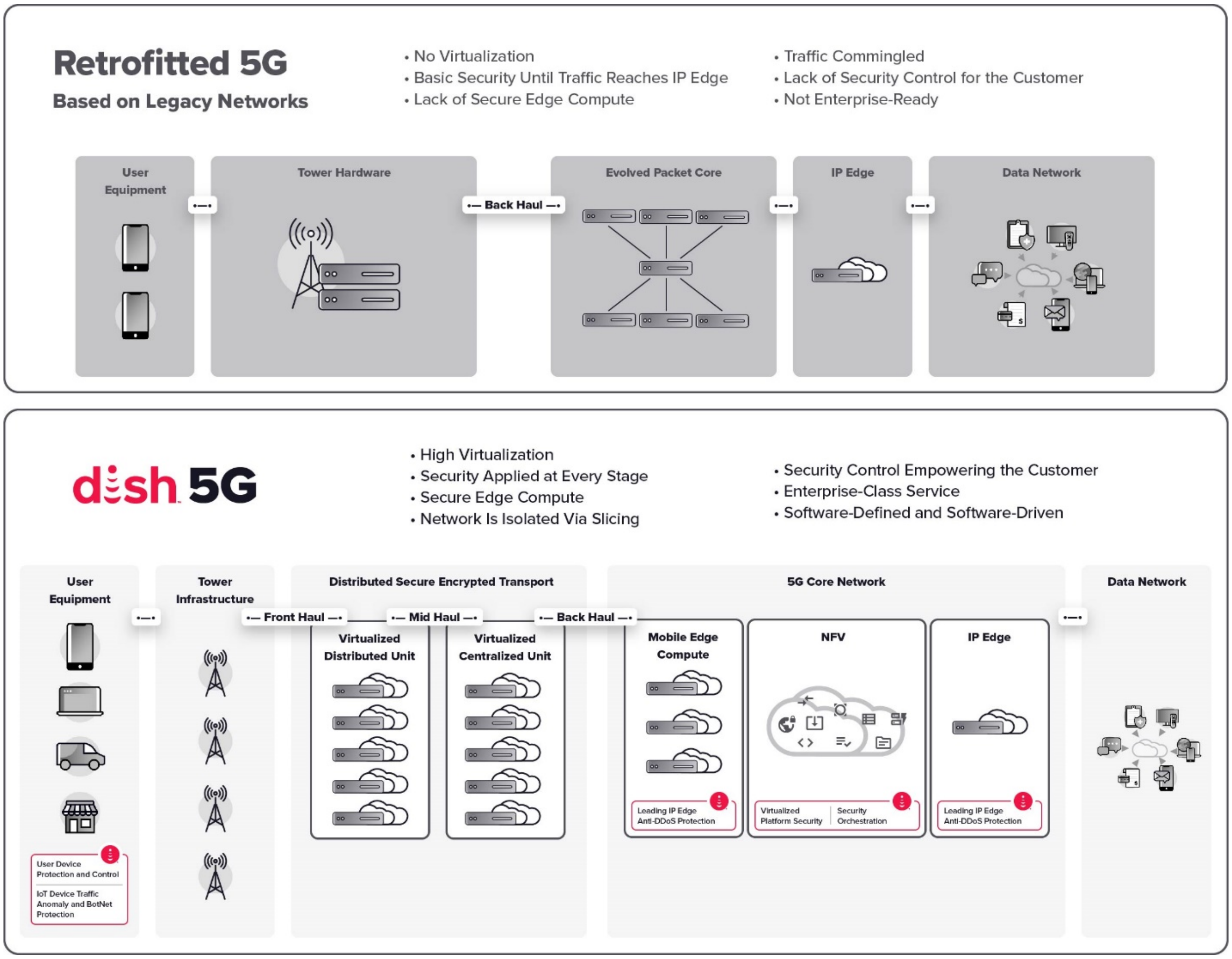
Figure 1. Network Slicing



In addition to 5G network slicing, service orchestration delivers customized, end-to-end services. Through the orchestration process, DISH will define the customized configurations for customers' unique applications. Here, wide-ranging security capabilities will be added to ensure customers' data — both in motion and at rest — is safe and secure.

Finally, rules, workflows, and various physical components lie underneath the orchestration canvas before they are coupled together to form customer-specific network slices. As shown in Figure 2 below, DISH's secure architecture is better equipped to meet customer requirements and demands than traditional networks.

Figure 2. DISH 5G's Secure, State-Of-The-Art Architecture


Retrofitted 5G
Based on Legacy Networks
• No Virtualization
• Basic Security Until Traffic Reaches IP Edge
• Lack of Secure Edge Compute
• Traffic Commingled
• Lack of Security Control for the Customer
• Not Enterprise-Ready
User Equipment
Tower Hardware
Back Haul
Evolved Packet Core
IP Edge
Data Network
dish 5G
• High Virtualization
• Security Applied at Every Stage
• Secure Edge Compute
• Network Is Isolated Via Slicing
• Security Control Empowering the Customer
• Enterprise-Class Service
• Software-Defined and Software-Driven
User Equipment
Tower Infrastructure
Distributed Secure Encrypted Transport
Front Haul
Mid Haul
Back Haul
Virtualized Distributed Unit
Virtualized Centralized Unit
5G Core Network
Mobile Edge Compute
NFV
IP Edge
Data Network
User Device Protection and Control
IoT Device Traffic Anomaly and BotNet Protection
Leading IP Edge Anti-DDoS Protection
Virtualized Platform Security
Security Orchestration
Leading IP Edge Anti-DDoS Protection

End-to-End Security. The new capabilities offered by DISH's network will give customers superior data protection, security, and network reliability. By moving the processing of data out of the traditional data center to the edge of the network, we will deliver ultra-low latency required by new applications. The advantages are clear: secure edge computing, hardware and chip-based security, unprecedented customer control and a first-of-its-kind, enterprise-grade wireless infrastructure.

In particular, DISH's architecture provides end-to-end security, advanced threat visibility and secure function isolation. Through automation and orchestration, DISH's network will provide the highest level of security at the speed of system workloads, and the network will allow for confidential computing at the edge. Customers will have full security control from the outset, including flexible user plane protection (UPP), policy management and control with system-enabled self-healing, made possible by artificial intelligence (AI) and machine learning (ML) tools. DISH's network will support customers that require control over selected components of the RAN and core network functions. DISH is also adopting measurable, state-of-the-art security standards beyond those currently found in the industry, to provide a higher level of security for its customers. DISH has partnered with Nokia to provide end-to-end security and orchestration, from the physical hardware level to each application.

Firewall, Cloud and Container Security. DISH's network will utilize 5G-native, next-generation containerized firewalls. These firewalls include real-time threat correlation, 5G slice security and dynamic security enforcement and integrate a high degree of automation to manage security efficiently. With these services in place, DISH will be able to observe and control security across all network layers and locations, including the full stack of the containers and infrastructure, providing comprehensive protection. The Open RAN model ensures that DISH will be able to stay at the leading edge of security technology by working with best-in-breed security vendors now and in the future. DISH has chosen Palo Alto Networks, a cybersecurity leader, to deliver firewall innovation and enable the secure digital transformation of DISH's network.

V. THE COMMISSION SHOULD TAKE STEPS TO PROMOTE OPEN RAN ADOPTION IN THE UNITED STATES

Given the significant benefits of Open RAN, DISH provides the Commission with recommendations on "steps [that] are required to deploy Open RAN networks broadly and at scale."[5]

A. The Commission Should Support Robust Funding for Open RAN

The Commission should support Congress funding $1.5 billion into the Public Wireless Supply Chain Innovation Fund (PWSCIF) and $1.5 billion into the Multilateral Telecommunications Security

[5] NOI at ¶ 3.

Fund (MTSF).[6] The Fiscal Year 2021 National Defense Authorization Act authorized PWSCIF and MTSF, originally contemplated under the bi-partisan and bi-cameral USA Telecommunications Act. The PWSCIF, administrated by the National Telecommunications and Information Administration (NTIA), offers grants targeting the use of innovative technologies within the RAN. In the short term, these funds will propel research and development, job creation and the building of secure and trusted solutions domestically. In the long term, it is an investment in the creation of a diverse and robust supply chain that will persist for many years in the wireless industry.

B. The Commission Should Provide Carriers Additional Time to Deploy Open RAN

Carriers working to "Rip-and-Replace" currently installed equipment and services that Congress determined pose a national security risk to U.S. communications networks may not be able to do so with Open RAN solutions within the current one-year timeline. To promote adoption and deployment of Open RAN, the Commission should grant at least a twelve-month extension of the compliance deadline for any carrier that commits to replacing covered communications equipment with Open RAN solutions.

The Secure and Trusted Communications Act of 2019 (STCNA) provides a one-year period for program recipients to replace covered equipment; that clock runs from the date the Commission distributes reimbursement to such recipients.[7] But, Congress recognized that carriers may not be able to meet the one-year timeline associated with this program. The statute thus provides for both general and individual extensions of up to a year.[8]

Among other benefits, an extension will give wireless carriers the incentive to consider Open RAN solutions that will expand the telecommunications supply chain, promoting the security goals of

[6] Public Law No: 116-283 (enacted Jan. 1, 2021).

[7] Secure and Trusted Communications Act of 2019, 47 USC § 1603(d)(6) (2019).

[8] 47 USC § 1603(d)(6).

the law. Congress specifically contemplated this type of technology change in the statute.[9] DISH recognizes that carriers who choose to proceed with Open RAN solutions likely need additional time to ensure compatibility with existing non-Open RAN equipment and continuity of service for their customers. Congress contemplated challenges like this, and gave the Commission the authority to extend the general deadline by six months if it finds that "the supply of replacement communications equipment or services needed by the recipients to achieve the purposes of the Program is inadequate to meet the needs of the recipients[.]"[10]

In addition, granting an extension is consistent with Congressional requirements that the program create a level playing field for equipment and services. Congress made clear that the Commission must not disadvantage "virtual communications equipment, application and management software and services" as it implements the STCNA.[11] However, the one-year deadline, absent an extension, will disadvantage carriers seeking to implement new technologies that require more engineering analysis, undermining the goals of the law.

Accordingly, to ensure wireless carriers make replacement decisions based on security, cost savings, and performance criteria, rather than the expedience of selecting a legacy non-interoperable network, the Commission should grant program recipients that commit to Open RAN solutions, at least, an additional twelve months to complete the transition.

[9] H. Rpt. No. 116-352, at 11-16 ("The Committee expects the Commission, when implementing regulations described under this section, to preclude network upgrades that go beyond the replacement of covered communications equipment or services from eligibility; however, th*e Committee expects there to be a transition from 3G to 4G or even 5G-ready equipment in instances where equipment being replaced was initially deployed several years ago*." (emphasis added)).

[10] 47 USC § 1603(d)(6)(B)(i).

[11] 47 USC § 1603(d)(1)(B).

VI. CONCLUSION

DISH appreciates the Commission's efforts to support the growth of the Open RAN supply chain and encourages it to adopt the proposals provided herein.

/s/ Jeffrey Blum
Jeffrey H. Blum
Executive Vice President, External &
Legislative Affairs
DISH Network Corporation
1110 Vermont Avenue, NW, Suite 450
Washington, DC 20005
Jeffrey.Blum@dish.com
(202) 463-3703

April 28, 2021