Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC

In the Matter of	)	Docket No. 200521-0144
	)	
National Strategy to Secure 5G Implementation Plan	)	
	)	
	)	

COMMENTS OF MAVENIR SYSTEMS, INC.

Mavenir Systems, Inc. ("Mavenir")[1] submits these comments in response to the Request for Comments ("Request") by the National Telecommunications and Information Administration ("NTIA") released on May 28, 2020, which seeks input on the development of an Implementation Plan for the National Strategy to Secure 5G in the above-referenced docket.

On March 23, 2020, President Trump signed into law the Secure 5G and Beyond Act of 2020,[2] which requires the development of a strategy within 180 days of enactment[3] to ensure the security of next generation wireless systems and infrastructure. On the same day that this law was enacted, the Administration published the National Strategy to Secure 5G ("5G Strategy"). The Administration's 5G Strategy

[1] Mavenir is a U.S headquartered supplier of end-to-end mobile network solutions for LTE and 5G. Mavenir is owned by Siris Capital, a private equity firm based in New York, New York. Mavenir has been a pioneer and provider in the development and supply of virtualized platforms, already supplying many large scale virtualized core elements in the United States and globally for both LTE and 5G. Mavenir's portfolio includes the Radio Access Network (RAN) and 5G Core, as well as Voice and Video via IMS, enabling Mavenir to serve as a complete and secure 4G/5G Core and Radio Access Network ("RAN") end-to-end system provider.

[2] Pub. L. 116-129, 134 Stat. 223 (2020) ("Secure 5G Act").

[3] *Id.*, Section 3(a).

recognizes both the importance of 5G to the future prosperity and security of the United States as well as the risks and vulnerabilities that could be nefariously used by bad actors seeking to exploit 5G technology. In implementing the 5G Act and executing the 5G Strategy, NTIA is seeking to develop an Implementation Plan along four lines of effort, namely (1) facilitating domestic 5G rollout; (2) assessing the cybersecurity risks to and identifying core security principals of 5G capabilities and infrastructure; (3) addressing risks to U.S. economic and national security during the development of 5G infrastructure worldwide; and (4) promoting responsible global development and deployment of 5G. Mavenir addresses each of these lines of effort below.

I. The U.S. Should Facilitate Domestic 5G Rollout by Promoting U.S. Manufacturing of 5G Technology and Infrastructure in the U.S. by U.S. Headquartered Companies.

In order to facilitate the rollout of 5G domestically, the government should seek to widen the supply chain under the principles defined by OpenRAN and reduce the country's reliance on a small number of foreign-based companies who provide proprietary and expensive hardware-based equipment. Competition through market entry by U.S. suppliers who provide innovation, cost-effective and greater choices as well as secure alternatives to the closed and costly proprietary technology offered by foreign-owned vendors whether European or Chinese, is the key to lowering costs domestically, avoiding a foreign-owned domestic vendor duopoly, and positioning U.S. suppliers to compete internationally. The government can promote competition and assist U.S. suppliers by (A) supporting and incentivizing the adoption of interoperable open interfaces; (B) encouraging the manufacturing of low-cost, open interface (O-RAN) radios in the U.S. for global use, including the creation of volume and scale; and (C) supporting the development of low-cost semiconductor technologies that are used in radio RF manufacturing.

A. Support and Incentivize the Adoption of Open Interfaces

The U.S. should support and incentivize the adoption of interoperable open interfaces and OpenRAN technology both domestically and abroad. OpenRAN is disaggregated RAN functionality built using open and interoperable interface specifications between elements. This can be implemented in vendor-neutral hardware and software-defined technology based on open interfaces and community-developed standards. By encouraging open, interoperable interfaces based on a shared and transparent set of standards, the U.S. can create a more vibrant and secure 5G ecosystem. Vendors will have more opportunities to innovate, compete, and develop new network applications, as well as lower capital and operating expenditures for mobile operators. According to a 2019 paper by Strategy Analytics,[4] OpenRAN results in 40 percent lower capital expenditures and 34 percent lower operating expenditures for wireless carriers – a cost savings that will spur quicker 5G deployment, especially to traditionally underserved communities in the U.S.

B. Encourage the Manufacturing of Low Cost, Open Interface Radios in the U.S.

The U.S. should encourage the production of low cost, open interface radios for use in the U.S. and abroad. Today, radios (both open and closed interface) are manufactured overseas in Taiwan, Korea and China even though U.S. design capability exists domestically. The radios are then sold to foreign owned vendors such as

[4] "OpenRAN changes the Economics of RAN Infrastructure." *Mavenir*, Infographic, Jun. 25, 2020, https://mavenir.com/resources/infographic-openran-changes-the-economics-of-ran-infrastructure/?sf_action=get_data&sf_data=results&_sft_resource_type=infographic.

Ericsson and Nokia for resale in the U.S, again adding costs in the form of excess margin stacking and reinforcing the U.S. foreign-owned vendor duopoly. This is a fundamental weakness the U.S. faces in trying to win the race to 5G and keep its 5G networks secure. The U.S. needs low cost, U.S.-managed large volume manufacturers of radios because building radios in small quantities does not allow for scale to reduce pricing and compete globally. The inability to scale up to mass produce radios creates a market barrier to new entrants and limits U.S. growth and innovation. Scale is needed to achieve reduced cost targets and to help U.S. companies have a sustainable advantage and better compete globally where the U.S. can showcase its innovative solutions made possible through open interfaces that will allow for the design of customized 5G solutions for a variety of industry sectors and consumer facing purposes.

C. Assist with the Development of Low-cost Semiconductors

To ensure that the FCC has secure 5G networks, it must be certain that components used to build the infrastructure are secure. The security, integrity and ready availability of the semi-conductor chips play a critical role. Having U.S.-based manufacturing of semi-conductors will not only lower costs, but will make sure there is a ready supply while enabling oversight of production to strengthen security to U.S. standards. Recently, Taiwan Semiconductor Manufacturing Co., ("TSMC") announced plans to build a $12 billion semiconductor factory in Arizona, with construction to start next year. The plan not only brings semi-conductor manufacturing to U.S. soil, it is expected to create at least 1,600 high-tech jobs with production anticipated by 2024.[5] More importantly, the key component for manufacturing low cost radios (programmable gate arrays and ASIC derivatives) will be assured domestically and the U.S. will not risk being held hostage to future trade wars and national conflicts thereby providing certainty of an adequate supply chain. The U.S. must continue to encourage manufacturing of semi-conductors in the U.S. and should provide incentives for companies to locate manufacturing within the U.S.

D. Ensure Federal Funds Are Directed to Open RAN Solutions

The U.S. is a purchaser of radios and private wireless networks domestically for its federal offices and military installations and abroad for its military bases and embassies. Accordingly, the U.S. should create volume-based government procurement opportunities to ensure national security and in volumes large enough to leverage its purchasing power to create scale for Open RAN solutions.

In particular, with respect to replacing Huawei and ZTE equipment and services purchased by small rural carriers with federal funding, the U.S. should encourage the purchase of 5G equipment and services to future proof these networks and ensure security through open interfaces and Open RAN. Congress is poised to appropriate between $1 and $2 billion to small rural carriers serving fewer than 2 million subscribers to remove, replace and destroy Huawei and ZTE equipment utilized in their networks to fund the Secure Networks Act. Most of the equipment to be replaced is 3G or 4G LTE equipment. Allowing these carriers to upgrade to 5G as part of the replacement

---

[5] Pham, Sherisse, "Taiwan chip maker TSMC's $12 billion Arizona factory could give the US an edge in manufacturing." *CNN Business*, May 15, 2020, *see* https://www.cnn.com/2020/05/15/tech/tsmc-arizona-chip-factory-intl-hnk/index.html.

process, or at a minimum to be 5G ready, will set the stage to ensure that these rural networks, which will be critical for precision agriculture and rural telehealth, will be secure and able to protect and enhance the U.S. food supply, the oil and gas industry and sustainable energy production found in rural America.

In addition to working on the regulations to disburse the rip and replace funding, the Federal Communications Commission is working on another proceeding to fund 5G rollout in rural areas. The 5G Rural Fund has $9 billion to be distributed over a ten-year period for the deployment of 5G. That money stands to go further if open interfaces and Open RAN are utilized and spent on trusted U.S. based suppliers. Having the radios manufactured in time for rural wireless carriers to take advantage of the lower costs means more deployment of 5G across hard to serve areas.[6] Greenfield Mobile Network Operators (MNOs), like Dish Networks, will also benefit from a lower cost structure and the ability to future proof their networks as a result of deploying open interfaces and the increase competition that will result when more U.S. suppliers are part of the supply chain.

Other countries also need to replace Huawei and ZTE networks so that they can secure their communications infrastructure. The U.S. should work with the "Five Eyes" nations, the European Union and other democratic countries[7] to help solve the funding

[6] Mavenir, "Altiostar and Mavenir to Deliver OpenRAN Radios for US Market." *Press Release*, Jun. 11, 2020. *See* https://mavenir.com/press-releases/altiostar-and-mavenir-to-deliver-openran-radios-for-us-market/.
[7] "U.S., Brazil in talks on funding to buy 5G gear from Ericsson, Nokia: paper." *Reuters*, June 12, 2020, *see* https://www.reuters.com/article/us-brazil-usa-telecoms/u-s-brazil-in-talks-on-funding-to-buy-5g-gear-from-ericsson-nokia-paper-idUSKBN23J2P1.

issues related to the replacement of their Huawei and ZTE infrastructure using open interfaces and Open RAN.

II. The U.S. Should Assess the Cybersecurity Risks to and Identify Core Security Principals of 5G Capabilities and Infrastructure by Promoting Open Interfaces and Interoperability Through Adoption of Open RAN.

Deployment of Open RAN solutions will strengthen the security of U.S. 5G networks and prevent some of the risks that small rural wireless carriers are facing today.

A. Open RAN allows for secure open interfaces.

Open RAN reduces security risks. The open interfaces utilized for Open RAN are defined in technical specifications and provide a foundation and architecture for improving security. Although wireless carriers are procuring and integrating Open RAN network elements in new ways, wireless carriers bring the same expertise, diligence and requirements for security and resilience to these environments. With 5G, Open RAN brings new capabilities and control points that enable suppliers, test equipment manufacturers and wireless carriers to assess and to manage security risks. Open RAN provides the framework for the communications network ecosystem to align on the shared understanding of security requirements and to tailor security requirements at a more granular level than has been possible before. Open RAN's open interfaces are defined transparently in technical standards bodies, built on battle-hardened methods for protecting the cloud, and rooted in proven hardware and software virtualization technology.

B. 5G networks are introducing advanced security features that mitigate the risk of security breaches.

5G networks utilizing open standards have introduced advanced security features, which include enhanced subscriber privacy, state-of-the-art secure communications, and secure intra and inter operators' communications. Enhancements to the 5G networks come in multiple areas, including:

1. Standards driving transparent and vetted security, interoperability and trust;
2. Cloud architecture ensuring resilience, scalability and segmentation and the introduction of Mobile Edge Computing (MEC); and
3. Micro segmentation, containerization and virtualization providing enhanced security and isolation from the hardware up.

These advanced security features will protect network users across all sectors of business as well as leisure use of the 5G networks.

1. Open interface standards drive interoperability, trust and innovation.

Building open, interoperable and standards-based 5G networks has encouraged innovation and competition among diverse companies worldwide to enable greater security for 5G. Standards bodies such as 3GPP, GSMA, ETSI and the O-RAN Alliance help grow the ecosystem by enabling new and existing suppliers and wireless carriers to rapidly align on security requirements. These standards bodies are actively developing new test procedures and methods to ensure that network components support all of the security and performance requirements of network users.

Open standards help both network users and wireless carriers align on and demonstrate successful implementation of security requirements. Open standards foster more 5G solution suppliers to wireless carriers, who can offer a common solution to many operators, instead of developing unique, one-off solutions to support the hidden protocols and low levels of security requirements for a specific carrier when the interfaces are proprietary. More importantly from a security standpoint, wireless carriers and suppliers can coordinate new information about threats, vulnerabilities and exploits, allowing greatly accelerated development and deployment of risk mitigation to prevent or give warning of potential security breaches. The OpenRAN and 3GPP standards have focused on security aspects and multiple enhancements have been made to the specifications to improve network security in 5G. Using OpenRAN allows multi-vendor solutions and ensures that no single vendor locks the MNO into a certain technology choice and roadmap that ultimately would give end-to-end control of the telecom network to that single vendor.

2. Cloud architecture contributes to the security of 5G networks.

5G is designed to be built on a cloud architecture – the same cloud architecture that is the foundation of today's IT companies, internet and the public cloud. All security features that have been developed and enabled in IT and the cloud industry today can be applied to the telecom networks now running in the cloud. The dynamic nature of cloud computing makes it scalable and more resilient. Cloud architecture allows for rapid, standards-based deployment of infrastructure as needed. For example, in response to live traffic on the 5G network, workload-specific encryption or authentication capabilities might be required. With a cloud architecture, automated sensors can immediately detect the need and automatically provision and deploy these capabilities as needed. 5G cloud architecture also facilitates improved network segmentation, allowing grouping and separation of security sensitive network functions. The same architecture allows the deployment and lifecycle management of entire use cases using "network slicing." Because a network slice is effectively a complete end-to-end mini network, each slice will include security protocols appropriate to its own requirements and can be developed and deployed as a slice and kept separate from the rest of the 5G network.

3. Mobile Edge allows security features to be implemented in the RAN.

Mobile Edge, or Multi Access Edge Computing (MEC), includes elements that are traditionally part of the core network. As critical functions migrate to the Mobile Edge, carriers are implementing new security functionalities to ensure a highly secure mobile network, including:

a. Distributed Denial of Service (DDoS) detection and mitigation at the edge of the network to enhance the ability to respond to attacks and reduce potential broader network impact;

b. Stronger encryption of the over-the-air interface and encryption of each device's IMSI to further secure consumer device-specific information; and

c. Security edge protection proxy that will mitigate vulnerabilities in prior technology (*e.g.,* SS7 and Diameter) and attacks when subscribers are roaming between different wireless carriers' networks.

Additionally, the deployment of identity and access management (IdAM) and strong authentication are critical. IdAM is a means of managing a given set of users' digital identities and the privileges associated with each identity. These identities are then used as a means to enable strong authentication to access key capabilities in the network, supporting concepts like micro-segmentation and containerization. As such, the 5G IdAM system must be part of the next generation security and identity platform as a requirement for the 5G cloud-native modern identity security solution. By requiring 5G IdAM as a standard protocol, the U.S. will ensure its domestic 5G networks are secure.

OpenRAN is about open interfaces and providing a foundation and architecture for improving security, widening the supply chain and growing a vibrant ecosystem. By fostering the Open RAN ecosystem and incentivizing wireless operators to deploy OpenRAN, the U.S. government will improve 5G security both domestically and internationally. By working with the "Five Eyes" nations, the European Union and other like-minded countries, the U.S. can also foster the deployment of OpenRAN internationally and then together with these friendly countries promote wider spread adoption of OpenRAN.

III. The U.S. Should Address Risks to U.S. Economic and National Security During the Development of 5G Infrastructure Worldwide by Creating Funding Sources for Trusted U.S. Infrastructure and Service Companies to Compete Domestically and Internationally.

The U.S. should support and prioritize U.S. alternatives to foreign-based equipment providers by encouraging OpenRAN deployments domestically by directing that federal funding be set aside for such deployments; establishing federal grant programs for research and development; and creating tax incentives and other financing incentives to stimulate domestic manufacturing of radios and components that support OpenRAN. Directing federal funds dedicated to deploying mobile broadband –including the $1 billion+ recently authorized to rip and replace Huawei and ZTE equipment pursuant to the Secure and Trusted Communications Networks Act of 2019[8] – to U.S. companies that utilize OpenRAN technology for end-to-end 5G network solutions will ensure that the networks are secure and future proofed. Mavenir notes that Chairman Pai has

[8] Pub. L. 116-124, 133 Stat. 158 (2020) ("Secure Networks Act"), Section 4(d)(5)(B).

already requested that Congress appropriate as much as $2 billion to accomplish this effort.[9]

In addition, establishing and funding a grant program to help advance the deployment of open and interoperable interfaces in the U.S. and grow the U.S. supply chain through the passage of H.R. 6624[10]/S. 3189[11], the USA Telecommunications Act, or Sec. 501 of the Intelligence Authorization Act for Fiscal Year 2021 approved by the Senate Select Committee on Intelligence on June 3, 2020[12], will facilitate the ability of the U.S. to gain ground in the race to develop and deploy 5G solutions.

Encouraging the manufacturing of open interface, low-cost radios in the U.S. through financing assistance for research and development and the building of manufacturing facilities in the form of grants, low-cost loans, federal credit lines, tax incentives or credits or supporting the creation of public-private partnerships with U.S. headquartered companies would facilitate a secure domestic supply chain of this essential 5G component for U.S. mobile operators.

---

[9] Letter from Federal Communications Commission Chairman Pai to Sen. John Kennedy and Sen. Chris Coons (March 14, 2020) at p. 3. *See* https://img.lightreading.com/downloads/fccthing.pdf.

[10] House Committee on Energy and Commerce, "Bipartisan Members Introduce Bill to Promote Competitive and Secure 5G Equipment." *Press Release*, Apr. 24, 2020. *See* https://energycommerce.house.gov/newsroom/press-releases/bipartisan-members-introduce-bill-to-promote-competitive-and-secure-5g

[11] Office of U.S. Senator Marco Rubio, "Rubio, Warner, Burr, Colleagues Introduce Bipartisan Legislation to Develop American 5G Alternatives to Huawei." *Press Release*, Jan. 14, 2020. *See* https://www.rubio.senate.gov/public/index.cfm/2020/1/rubio-warner-burr-colleagues-introduce-bipartisan-legislation-to-develop-american-5g-alternatives-to-*huawei*.

[12] U.S. Senate Committee on Intelligence, "Senate Intelligence Committee Passes Intelligence Authorization Act." *Press Release*, Jun. 3, 2020. *See* https://www.intelligence.senate.gov/press/senate-intelligence-committee-passes-intelligence-authorization-act.

Mavenir also recommends that the U.S. recognize and publicly support U.S. companies that are already competing and successfully delivering 5G solutions globally, encouraging adoption of OpenRAN to further grow the supply chain rather than seeking to perpetuate the problem by investing in foreign-owned vendors.[13] For example last week, Mavenir and Altiostar announced a joint initiative to deliver a wide portfolio of radios based on OpenRAN principles for the U.S. market. Both companies will be supporting the development of radios through third party OEM's that will be based on O-RAN open interfaces to address the radio frequencies licensed to Tier-1 and Regional/Rural operators in the US.[14] These actions should be lauded and incentivized by the U.S. at every opportunity.

IV. The U.S. Should Promote Responsible Global Development and Deployment of 5G by Ensuring US Participation in Global Standards-Setting Bodies.

By encouraging participation of U.S. stakeholders in standard-setting bodies, the U.S. can ensure that when U.S. carriers deploy equipment and services for 5G

[13] Benner, Katie, "China's Dominance of 5G Networks Puts U.S. Economic Future at Stake, Barr Warns." *New York Times*, Feb. 6, 2020, ("[Attorney General] Barr agreed that too few companies were making 5G equipment; Nokia and Ericsson are the only other global competitors. [Barr] said that proposals had already been floated to address this problem, including the possibility that a consortium of private American and allied companies could put financial might "behind one or both of those firms" to make them more competitive and guarantee their staying power."). *See* https://www.nytimes.com/2020/02/06/us/politics/barr-5g.html. *See also* Dano, Mike, "Here's why Mike Pompeo wants a watered-down open RAN." *LightReading*, Jun. 10, 2020, https://www.lightreading.com/5g/heres-why-mike-pompeo-wants-a-watered-down-open-ran/a/d-id/761601, (Secretary of State Pompeo attempted to broker a watered-down version of Open RAN dubbed "ION" to gain support from entrenched foreign vendors who fear revenue losses that will result from the competition Open RAN deployment brings).

[14] Mavenir, "Altiostar and Mavenir to Deliver OpenRAN Radios for US Market." *Press Release*, Jun. 11, 2020. *See* https://mavenir.com/press-releases/altiostar-and-mavenir-to-deliver-openran-radios-for-us-market/.

networks, from whatever source, the equipment and services meet the standards of speed and security that Americans deserve. This notion has already been supported in both the House and the Senate. The House, on January 8, 2020, passed the Promoting United States Wireless Leadership Act of 2020.[15] H.R. 4500 requires the Assistant Secretary of Commerce for Communications and Information (Assistant Secretary) to assist trusted companies and other relevant stakeholders with participating in organizations[16] that set standards for 5G networks and for future generations of wireless communications networks, specifically for wireless devices and related equipment.[17] It also mandates that the Assistant Secretary equitably offer technical expertise to companies to aid participation in such standard-setting bodies.[18] The Senate introduced a companion bill, that outlines these same requirements.[19]

U.S. participation in standard-setting for 5G networks needs to be a priority. As the deployment of 5G networks has already begun, it is important that carriers and trusted vendors are part of the standard-setting, and resultant patent process due to their expertise and practical experience with U.S. communications networks. By participating in the global standard-setting processes for 5G networks, the U.S. can further ensure consistency, and security in U.S. communications networks and, given

---

[15] "Promoting United States Leadership Act of 2020," H.R. 4500, 116 Cong. (2020) ("H.R. 4500").

[16] *Id*., Section 2(b) (cites standard-setting organizations such as the International Organization for Standardization, the 3rd Generation Partnership Project (3GPP), the Institute of Electrical and Electronics Engineers, and any standard-setting body accredited by the American National Standards Institute or the Alliance for Telecommunications Industry Solutions).

[17] *Id*., Section 2(a)(1).

[18] *Id*., Section 2(a)(2).

[19] "Promoting United States Leadership Act of 2020," S. 3311, 116 Cong. (2020) ("S. 3311").

that communications networks are increasingly becoming globalized, provide greater transparency for U.S. mobile operations when dealing with a trusted vendor, no matter the origin of the equipment. Finally, Mavenir recommends that the U.S. host these standards meetings on U.S. soil and allow foreign participants to travel to the U.S. to participate. In the past, the U.S has not allowed some foreigners to travel to the U.S. to participate, which has driven the meetings to be held in foreign countries that then indirectly drive up the cost of participation by U.S. stakeholders.

Respectfully submitted,

By: */s/ Pardeep Kohli*

Pardeep Kohli, CEO
Mavenir Systems, Inc.
1700 International Parkway
Richardson, TX, 75081 USA
pardeep.kohli@mavenir.com
469-916-4393

June 25, 2020