Introduction

Marvell Technology Inc. ("Marvell") appreciates the opportunity to respond to NTIA's request for comment on implementation of the Public Wireless Supply Chain Innovation Fund.

Marvell is a leading supplier of high-performance standard and optimized infrastructure semiconductor and cybersecurity solutions, for the cloud data center, carrier infrastructure, enterprise, and automotive markets. Marvell's solutions empower the data economy with essential technologies for data centers and wireless networks from the radio to the core.

Marvell shares the vision and mission of expanding broadband access through building an open RAN infrastructure. Marvell has been a front-runner in promoting policies, investing in research, and driving design and development of such infrastructure [1],[2].

To that end, in the following sections, Marvell provides comments on:

- State of the Open RAN industry
- State of the Open RAN standards
- Suggestions regarding funding prioritization

State of the Open RAN 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?

Operators in close collaboration with Open RAN ecosystem partners including hardware vendors, software vendors, and system integrators have launched Open RAN-based 5G networks and services. Mass commercial deployment is the next step.

Major operators across the globe promote the open and interoperable architecture as specified by ORAN Alliances[3],[4],[5]. While the ecosystem has made great progress in adopting such an interoperable architecture, the mass commercial deployment of Open RAN will happen only when its CAPEX and OPEX costs, network performance, as well as user experience are at least as good as traditional network infrastructure.
The underlying network infrastructure and particularly, semiconductor components optimized for RAN play a key role in meeting the power efficiency, performance, and security requirements of the RAN networks. Among those, the use of advanced technologies nodes (5nm and beyond) has been instrumental in optimizing power consumption

[1] https://www.marvell.com/company/newsroom/marvell-joins-open-ran-policy-coalition.html
[2] https://www.marvell.com/company/newsroom/marvell-advances-no-compromise-5g-open-ran-with-partners-at-mwc-2022.html
[3] https://www.verizon.com/about/news/verizon-deploys-more-8000-vran-cell-sites
[4] https://www.fcc.gov/ecfs/file/download/2022-03-16%20DISH%20Ex%20Parte%20ORAN%20GN%20Docket%20No.%2021-63.pdf?folder=103161155918353
[5] https://www.vodafone.com/news/technology/vodafone-samsung-cooperate-marvell-accelerate-open-ran-performance-adoption

and reducing OPEX costs. Such semiconductor solutions are the cornerstones of today's deployed 4G and 5G radio networks worldwide. New, innovative features must be introduced in the next generations of silicon to address the unique challenges of Open RAN, while pushing the technological envelope to exceed the network performance and power efficiency of existing networks. US industry must invest in latest technology nodes and optimized silicon solutions that could close the technology gap in terms of power-efficiency, performance, and cost.

Another key hurdle for the ecosystem to overcome is to charter the business-model for end-to-end system integration, and life-cycle management. Operators will not take ownership of the end-to-end system deployment and maintenance; it is up to the Open RAN ecosystem to provide a diverse and interoperable alternative. As the RAN ecosystem migrates to an open architecture, it creates opportunity for hyperscalers and server vendors who have the technology leadership and scale to close the technology gaps, influence the operators, and accelerate the commercialization of Open RAN[6]. These vendors will help the Open RAN ecosystem by not only providing the hardware infrastructure, but also by pre-certifying and pre-integrating multi-vendor components and making the Open RAN easy to be adopted.

In the following, we provide recommendations that can accelerate the commercial adoption of the Open RAN.

Marvell recommends funding research, design and development of O-CU, O-DU and O-RU silicon components that support ORAN standards and meet the power efficiency, security, bandwidth, reliability, and resiliency requirements of 5G and 6G technologies.

The superior speed and reduced latency features of 5G technology has created the platform for new use cases with 1000x higher traffic volume and 5x lower latency. The infrastructure components are to meet this higher bandwidth and faster transport requirement while considering sustainability and power efficiency aspects of the whole ecosystem.

The mass commercial deployment of Open RAN depends on the power efficiency, network performance and end-to-end quantum-resistance security of its infrastructure and software components. Solutions that are not competitive in terms of performance, power efficiency, and security would not be able to transition from proof-of-concept trials to mass deployment. As such, optimized silicon components are key enablers of global commercial deployment for Open RAN ecosystem.

Marvell recommends industry partners make a joint commitment to adopt the disaggregated architecture defined by ORAN Alliance. As such, all the comments in this document refer to the disaggregated architecture defined in the ORAN Alliance architecture specification[7]. The key components in the ORAN architecture are:

- *O-CU (O-RAN Central Unit*): O-CU is a logical node hosting User Plane and Control Plane. The existing state-of-the-art O-CU solutions are optimized to address Open RAN's computational capacity, networking capabilities, and data transport capability requirements.

  The commercial grade O-CU solutions must use dedicated hardware accelerators for zero-touch packet processing and data transport. They need to provide end-to-end security through Hardware Security Modules ("HSMs") using hardware, cloud and/or embedded technologies for secure-boot as well as dedicated hardware accelerators for MAC-Sec and IP-Sec. They must be equipped with hardware and software enhancement features for emerging Machine Learning (ML) and Artificial Intelligence (AI) use cases. Their network interfaces should be optimized and secured for upcoming high bandwidth, and high throughput use cases.

[6] https://www.nokia.com/blog/the-collaborative-advantage-nokia-and-partners-delivering-best-in-class-cloud-ran-solutions/

[7] "O-RAN.WG1.O-RAN-Architecture-Description-v07.00 @ https://www.o-ran.org/specifications"

- *O-DU (O-RAN Distributed Unit):* O-DU is a logical node hosting RLC/MAC/High-PHY layers. The ever-increasing bandwidth requirements of 5G and emerging 6G technologies along with ultra-reliability and low latency requirements of new use cases (including XR/VR, smart cities, autonomous driving, and remote surgery) require optimized silicon solutions for L1 (physical layer) signal processing. The existing optimized O-DU solutions use COTS ARM/x86 servers for RLC and MAC processing and offload the High-PHY signal processing to the L1 accelerator cards. The O-DU components must also have built security features for secure boot (HSM using hardware and/or embedded) as well as hardware acceleration for MAC-Sec and IP-Sec.

- *O-RU (O-RAN Radio Unit):* O-RU is a logical node hosting low-PHY, beamforming and RF processing. 5G technology uses a wide range of approaches to increase the network capacity, including Massive MIMO, wider frequency bandwidths in sub-6GHz band, as well as above 6GHz (also called millimeter Wave, mmWave, or FR2). The complexity of O-RU solution varies in frequency bands and antenna configurations. Particularly, the RU configurations supporting Massive-MIMO and mmWave are quite complex and often incorporate integration of multiple analog and digital components. The mass deployment of such solutions requires multiple silicon components for RF processing, data conversion, advanced beamforming, and digital signal processing. All these components must be equipped with HSM (hardware and/or embedded) and meet the standard end-to-end security requirements. Further, the end-to-end integration, testing, and software development of the system requires significant capital investment.

The cost of design and development of such complex silicon solutions are quite significant, in the order of hundreds of millions of dollars. Without sponsorship from the government or a committed customer, individual companies are reticent to make such an investment. With NTIA's leadership and funding through the Wireless Innovation Fund, semiconductor companies can provide the required silicon components that will meet the bandwidth, reliability, and latency requirements of the emerging 5G use cases.

For all these offerings, investment in research, design, and development of 5nm (and beyond) silicon design and IP is imperative. With NTIA's support, the private sector will be able to provide best-in-class silicon components with increased power and spectral efficiency for Open RAN infrastructure and serve the global economy by increasing capacity and throughput, and enhancing the end-user's experience.

Marvell recommends NTIA to prioritize funding RAN software development

One of the key challenges the Open RAN ecosystem faces is the lack of mature open-source software solutions for wireless protocol stacks available to the wider software ecosystem. Examples of missing software blocks include L1 software, especially of blocks that experience significant change between 4G, 5G, and likely 6G, and massive MIMO acceleration algorithms for optimal beam selection. ORAN-compliant APIs and standard interfaces are another area for the US software industry must continue to invest. Current focus on plugfests and other interoperability tests at the box level are very hardware-centric and are generally not in the best interest of US companies.

Further, Protocol stack and software solutions need significant additional investment to reach the maturity and reliability level that is needed in a commercial-grade deployment.

With NTIA's support, the private sector could expand its investment to software development and facilitate faster adoption of Open RAN solutions.

State of the Open RAN Standardization

7. Are the 5G and open and interoperable RAN standards environments sufficiently mature to produce stable, interoperable, cost-effective, and market-ready RAN products?

Marvell believes standardization is mature-enough for product development. Further, Marvell recommends industry partners align their product development with the ORAN Alliance and 3GPP standard specifications.

Standard bodies such as 3GPP and ORAN Alliance have made great progress in defining the disaggregated RAN architecture and standard interfaces between components of the RAN network. A disaggregated architecture with standard interfaces is modular and could incorporate components from different suppliers. Such a diversity would create a competitive ecosystem where suppliers of all sizes could participate, and operators and end users would benefit from competitive price and performance offerings. To accelerate adoption of Open RAN, the ORAN Alliance has prioritized releasing the Minimum Viable Plan ("MVP") standard specification. The MVP standard specification is mature-enough to be used for commercial deployments and is available to be used as reference by the ecosystem. We urge the ecosystem to adopt MVP approach as once the MVP solution is deployed, the industry will be able to improve its offerings using the lessons from the MVP deployment.

The standardization process is certainly not a one-time task. Standardization bodies will continue to address the evolution of technology and publish incremental releases as required.

Questions on Trials, Pilots, Use case and Market development

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?

a. What kinds of testbeds, trials, and pilots, if any, should be prioritized?

Marvell recommends "Open and Interoperable" architecture and advises against prioritizing "plug-and-play" proof of concepts

Marvell sees the urge to differentiate between an open and interoperable infrastructure and a fully modular/plug-and-play architecture. Marvell promotes an Open and Interoperable infrastructure for RAN. In such an infrastructure, components, interfaces, and associated APIs are well defined. The interoperability and network resiliency are addressed through clear life-cycle management standards and certification processes. This is quite different in nature from a plug-and-play architecture.

The migration to Open RAN will be a gradual process where at each phase only a subset of the components of the network will be replaced with Open RAN compliant components. Full replacement of nation-wide network equipment in single phase is neither practical nor economically feasible. The integration and interoperability process must ensure that the end-to-end network continues to meet the performance and resiliency requirements. This can be met via catalogue-based interoperability testing and integration. Marvell recommends NTIA to prioritize funding the "open and interoperable" solutions. These solutions are practical enablers of vendor diversity and mass commercial deployment of Open RAN.

15. How might existing testbeds be utilized to accelerate adoption and deployment?

Marvell recommends leveraging the existing test-bed infrastructure to the extent possible

The key challenges highlighted in 5G Open RAN rollouts are technology readiness, cost, and integration ownership. These key challenges should be the top priorities for Open RAN ecosystem to address. Further, many of the innovation ideas require testing at a modular or sub-system level. Such technologies have taken advantage of the existing test-bed facilities that do not have end-to-end testing facilities but are well-equipped to test specific areas of the network architecture. The modularity of ORAN architecture is indeed one of the key factors in the ORAN Alliance and 3GPP test specification developments. While there is value in a widely open, end-to-end test-bed facility, it is not a "must-have" and a prerequisite for the commercial deployment of Open RAN. We recommend leveraging the existing facilities and modularity of Open RAN architecture to the extent possible.

Security: status and required future advancements

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?

a. What role should security reporting play in the program's criteria?

b. What role should security elements or requirements, such as industry standards, best practices, and frameworks, play in the program's criteria?

Marvell recommends NTIA to fund Open RAN related research, design, and development of quantum-resistant, hardware security module (HSM), and software/service assurance security solutions.

State of Open RAN Security Standards and the Industry:

The ORAN Alliance and particularly "Working Group 11" within the Alliance ("W11") has made great progress in identifying potential risks for Open RAN architecture and providing solutions to mitigate such risks[8],[9],[10]. The W11 Security Requirement Specification published by ORAN Alliance provides a comprehensive set of requirements and security controls that are designed to address identified risks particularly for "Life Cycle Management" of Open RAN architecture. Standard bodies continue to assess new threats and provide recommendations to mitigate such security threats.

Open RAN solution providers have commercial-ready security solutions for the 5G and Open RAN architecture, and security risks need not prevent near-term Open RAN deployment. Features such as secure boot, key protection via hardware HSM and/or embedded Hardware Security Modules ("eHSM"), IP-Sec, and MAC-Sec are only a few examples of security features available to Open RAN ecosystem. Hardware Security Modules deployed in today's hyperscale cloud datacenters are state-of-the-art with respect to encryption keys in today's environment. The funding will accelerate and extend research towards next generation quantum-resistant hardware security modules

[8] "O-RAN Security Protocols Specifications 4.0 @ https://www.o-ran.org/specifications"
[9] "O-RAN Security Requirements Specification 4.0@ https://www.o-ran.org/specifications"
[10] "O-RAN Security Threat Modeling and Remediation Analysis 4.0@ https://www.o-ran.org/specifications"

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

Open RAN security research, design, and development recommendations:

As Open RAN technology advances, new security threats will arise, and continuous investment in design and development of security solutions must be a priority. Here we address protections for predictable Open RAN threats.

Post-quantum cryptography and quantum-resistant algorithms capable of withstanding the threat of a future quantum computer have been studied by many organizations. The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) selected the first group of quantum-resistant algorithms in 2022. Robust long-term security will require Open RAN solutions including software tools and silicon components with native quantum resistance support. The standards and algorithms supporting such standards are still evolving and the Open RAN ecosystem must invest in design, development, and deployment of these solutions.

5G and Open RAN standards require pre-shared keys and PKI digital certificates. These keys/certs must be secured in all the Open RAN O-CU, O-DU, and O-RU solutions. Robust long-term security requires Open RAN key management solutions with keys anchored in hardware based HSM solutions including cloud-HSM, multi-cloud HSM, and/or embedded HSM (eHSM). Multi-cloud compatible HSM key management approaches will provide greater flexibility for carriers and telecommunications companies over the long term, so should be encouraged.

Open-source software running in virtual machines or docker containers require additional security infrastructure in Open RAN. Also, Cloud Service Provider ("CSP") and other solutions may offer more flexibility and a lower entry threshold via leased HW/SW components, instead of purchased. HSM usage need be mandated for keys securing services, including those that may spin up/down.

Open-source and commercial off the shelf software will ensure competition, interoperability, and ease of use in Open RAN. The security of these codes is paramount. Code and containers must be signed and authenticated, bound to the developer/publisher. The most critical secret signing keys must be contained within the strongest boundary, like a NIST FIPS 140-3 level 3 hardware HSM.