Responses to Additional Questions for the Record
John Baker
Senior Vice President, Business Development
Mavenir

U.S. House Committee on Energy and Commerce
Subcommittee on Communications and Technology
"Strengthening American Communications Leadership with Open Radio Access Networks"
Hearing Held January 17, 2024

In response to the Honorable Randy Weber (R-TX):

The O-RAN Alliance is a global organization comprised of mobile operators, suppliers, research institutions, academia, and governmental bodies. The Alliance's "mission is to reshape the RAN industry towards more intelligence, open, virtualized and fully interoperable mobile networks."[1] The Alliance operates in compliance with World Trade Organization (WTO) principles for the development of international standards, including transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and development dimension.[2] The Alliance conducts its work based on consensus, so that members can raise objections and curtail any efforts that are deemed counter to the organization's purpose of advancing open and interoperable specifications.[3] In recent years, the National Telecommunications and Information Administration (NTIA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) have joined the O-RAN Alliance, giving each agency a seat at the table and importantly, a vote on matters before the Alliance.

Open Testing and Integration Centers (OTICS) are run independent of the O-RAN Alliance and serve as open, vendor-independent, and impartial working centers for companies to test products and solutions.[4] Any O-RAN Alliance member (operators) and/or contributor (supplier) that is vendor neutral can apply to host an OTIC, and decisions related to testing and product confidentiality are made between the OTIC and the supplier. However, OTICs are not required to be used for interoperability testing for Open RAN, and operators and suppliers are free to choose to test their products in an OTIC or in other available laboratories or testing sites. Mavenir uses the CableLabs/Kyrio OTIC, which is located in Colorado, and which was selected twice by the Department of Defense and NTIA to host the agencies' joint 5G Challenge.[5] Mavenir also has our own dedicated lab in

[1] See https://www.o-ran.org/about
[2] See "Governance of O-RAN Alliance e.V. in Compliance with WTO Principles," (July 2023), available at: https://assets-global.website-files.com/60b4ffd4ca081979751b5ed2/64bee579b5449cafb9f0f889_Governance%20of%20O-RAN%20ALLIANCE%20e.V.%20in%20Compliance%20with%20WTO%20Principles-v02.pdf
[3] O-RAN Alliance Members can participate in any working group. Decisions in a working group are made by consensus, but if consensus cannot be reached, a vote can be called by the working group's co-chair. The principles of impartiality and consensus do not impose a requirement of unanimity except that before a vote is called, each contributor has had the chance to participate in the development of the specification and to express their views. The approval of specifications requires a two-thirds majority vote. No particular group (neither by country nor by founding member or otherwise) has a blocking majority. No veto rights exist, and no representation body (including the Executive Committee) can refuse to forward specifications once they are approved by working groups and the Technical Steering Committee.
[4] See https://www.o-ran.org/testing-integration
[5] See https://kyrio.com/cablelabs-partners-with-kyrio-to-serve-as-5g-2023-host-lab/

Richardson, Texas where we test our products and interoperate with other suppliers. We also test in operator-controlled laboratories.

As I testified before the committee, a certification process for Open RAN is needed so that credible, trusted, third party organization(s) can attest as to whether products meet the minimum requirements to be called Open RAN. It is essential to have this certification to ensure individual suppliers do not lock an operator/country to a single supplier solution that does not support fully the O-RAN specified interfaces. To restate, you only have Open RAN when you have demonstrated interoperability with multiple vendors.

In response to the Honorable Debbie Dingell (D-MI)

Open RAN, which stands for Open Radio Access Network, plays a significant role in enhancing the security of wireless networks. Open RAN contributes to making wireless more secure in a number of ways, including:

1. Vendor Diversity: Open RAN promotes vendor diversity by allowing operators to mix and match equipment from different vendors. This reduces the reliance on a single vendor and mitigates the risk of vulnerabilities or backdoors being exploited by malicious actors. Accordingly, it is critical that deployed Open RAN solutions be certified to have the proven mandatory open and interoperable interfaces.
2. Interoperability: Open RAN requires interoperability between different hardware and software components. By adhering to open standards, it ensures that various components from different vendors can seamlessly work together. This reduces the chances of vulnerabilities or security gaps caused by incompatible systems.
3. Open Standards: Open standards improve security by avoiding closed, proprietary systems that might have limited transparency and could hide vulnerabilities.
4. Enhanced Visibility, Flexibility, and Control: Open RAN provides operators with greater visibility, flexibility, and control over their network infrastructure. This allows them to closely monitor and manage the network components, detect any potential security threats, and quickly respond to them.
5. Software-Defined Security: Open RAN leverages software-defined networking (SDN) and network function virtualization (NFV) concepts. This enables operators to implement security measures, such as firewalls, intrusion detection systems, and encryption, in a more flexible and dynamic manner. They can easily update or modify security policies as needed, enhancing the overall security posture.
6. Reduced Monoculture Risk: Proprietary systems often create a monoculture where a single vendor's technology dominates the market. This can be risky from a security perspective because if a vulnerability is discovered in that technology, it could potentially impact a large portion of the network. Vendor diversity helps mitigate this risk.
7. Community Collaboration: Open RAN encourages community collaboration and knowledge sharing among operators, vendors, and researchers. This collaborative approach facilitates the identification and mitigation of security vulnerabilities more effectively. It allows for peer reviews, security audits, and the development of best practices for securing Open RAN deployments.

It is important to note that while Open RAN provides significant advantages in terms of security, it is crucial to implement additional security measures and best practices to ensure a robust and secure wireless network.