CableLabs Comments on

National Telecommunications and Information Administration
Public Wireless Supply Chain Innovation Fund Implementation
[Docket No. 221202-0260]
RIN 0693-XC053

INTRODUCTION

CableLabs appreciates the opportunity to provide input to the National Telecommunications and Information Administration (NTIA) on the implementation of the Public Wireless Supply Chain Innovation Fund (Innovation Fund). CableLabs is heavily invested in research and development (R&D) in the Open RAN ecosystem and views the Innovation Fund as presenting a critical opportunity to make significant advances towards widespread adoption of Open RAN.

CableLabs' investment in Open RAN is driven by the potential benefits, namely a more diverse and competitive vendor ecosystem for radio access network components and more critically, Open RAN will increase the pace of innovation in both the radio access network and the applications enabled through Open RAN standardization.

These benefits are predicated on a vision for Open RAN that delivers both a secure and truly "plug-and-play" level of interoperability for the radio access network. The Innovation Fund's statutory goals, funding levels, and timing provide the opportunity to create real change and to help realize this vision for the Open RAN ecosystem in a time frame unattainable by the private sector alone. To this end, the Innovation Fund should be used to:

- Eliminate, or at minimum, materially reduce, operator-specific System Integration efforts/costs through common testing programs and infrastructure;
- Accelerate performance of Open RAN components/systems to put them on par with or ahead of traditional/legacy RAN systems;
- Ensure that Open RAN components and systems are designed and built with security from the start that matches or outperforms the security of a traditional RAN; and
- Drive harmonization and scale to establish a self-sustaining ecosystem through increased and sustained private sector investment.

Background on CableLabs

CableLabs was initially founded in 1988 to help coordinate and drive common network technologies for the cable industry and today, is the R&D and innovation lab for the global cable broadband industry. CableLabs is a U.S.-based, non-profit membership organization with cable broadband network operators in the U.S., Canada, Europe, and around the world.[1] Today, roughly half of CableLabs members are also mobile network operators and that

[1] https://www.cablelabs.com/about-cablelabs/member-companies

proportion is only growing. Based on this direction, CableLabs is increasingly active in the mobile industry, including various industry-led Open RAN initiatives.[2]

CableLabs is currently focused on developing and advancing access network technologies, namely wired – hybrid fiber coax and fiber to the premise; wireless – mobile/3GPP, Wi-Fi, and fixed wireless access; and the security of those networks and the equipment that attaches to them. These comments are the view of CableLabs as an R&D organization and do not reflect the views of member companies.

Current Work on Wireless Access Networks, Including Open RAN

Approximately half of CableLabs' resources are dedicated to the development of wireless network technologies, as our members see mobile services as a critical part of their future growth in the U.S. and around the world. After more than a decade of participating in wireless network standards activities, we have made significant mobile technology investments in innovation and test environments over the last two years. Our current capabilities in Open RAN development, integration, and interoperability are industry leading.

CableLabs is heavily engaged in the standards development process focused on wireless-wireline convergence and standards-based interfaces at 3GPP and open, standards based interoperability through compliance at O-RAN Alliance. It is important to note that Open RAN is not a new technology but is a new approach that standardizes interfaces that were previously closed and proprietary. The Open RAN approach can be applied to 5G, 6G, and beyond.

CableLabs' subsidiary, Kyrio, is the first O-RAN Alliance Open Testing and Integration Center (OTIC) in the Americas, and the only OTIC globally run by a neutral innovation center, not by a specific operator or vendor. As part of the O-RAN Global PlugFest Fall 2022, Kyrio and CableLabs hosted the *PlugFest in North America* that focused on multi-vendor O-RAN end-to-end systems under test; demonstrations of open central unit (O-CU) interoperability; and near-real-time radio intelligent controller (near-RT RIC) conformance testing.[3] Kyrio's testing capabilities are available on a continuous basis to any interested vendor that meets the O-RAN Alliance criteria.

In 2022, CableLabs was selected as the Host Lab for the NTIA and the Department of Defense's (DoD) 5G Challenge. The 5G Challenge was a first of its kind event focused on conformance-based interoperability as opposed to operator- or deployment-specific system integration-based interoperability. The results of last year's challenge exceeded expectations. Multi-vendor interoperability was achieved in a very short amount of time, five weeks instead of the six months, as typically experienced in a plugfest. The lessons learned during our work on the 5G Challenge inform these comments and our future R&D efforts in the Open RAN space. We

[2] Including 3GPP, Telecom Infra Project (TIP), O-RAN Alliance, Broadband Forum, WiFi Alliance, Wireless Broadband Alliance.

[3] *See* O-RAN ALLIANCE Advances Testing and Integration with Successful O-RAN Global PlugFest Fall 2022, https://www.businesswire.com/news/home/20221214005850/en/O-RAN-ALLIANCE-Advances-Testing-and-Integration-with-Successful-O-RAN-Global-PlugFest-Fall-2022

are pleased to be selected as the Host Lab for the 2023 NTIA/DoD 5G Challenge and are expanding test capabilities and resources to meet the goals of the 5G Challenge.[4]

The Future of Connectivity

In the future, consumers will be able to access the connectivity services they need, anywhere, seamlessly. The network will provide a simplified end-user connection and provide increased intelligence to manage those needs efficiently and economically. The virtualization of networks and Open RAN are a key elements and enablers to CableLabs' vision of common core, multi-access networks because Open RAN offers more flexibility on the architecture and deployment than a traditional RAN. To take advantage of a truly converged solution, networks must be comprised of elements that are as common and simple as possible. Open RAN provides this ability. In addition, the opening and standardization of interfaces and APIs will enable increased investment and innovation in RAN applications (e.g., xApps and rApps) further increasing the diversity of the ecosystem and creating new value for consumers and network operators, alike. As such, the Innovation Fund presents an unrivaled opportunity for NTIA to kick start critical R&D contributions to the adoption and deployment of standard and interoperable network elements that will build the future of connectivity. CableLabs looks forward to continuing the conversation with NTIA on how to effectively achieve the goals of the Innovation Fund.

RESPONSE TO SPECIFIC QUESTIONS PRESENTED IN THE REQUEST FOR COMMENTS

I. State of the Industry

Questions 1 and 1a: The full potential of Open RAN can be effectively realized under a healthy ecosystem driven by large-scale Open RAN deployments. However, key challenges to the success of Open RAN still must be addressed. These challenges fall into five areas: network deployment strategies, vendor ecosystem, performance, management, and investment.

The first, network deployment strategy, is the need for the wireless industry to move away from proprietary systems and proprietary system based "interoperability." For a network to truly comply with Open RAN goals and optimize the benefits, network systems should be built to comply with an agreed upon set of standards and specifications, creating a truly interoperable system where pieces of equipment can be plug-and-play and operators can change vendors without a meaningful level of risk. This is different than today when each operator directs equipment vendors to comply with a unique set of standards or specifications that inhibits true interoperability and increases the cost of repairs and replacement of RAN equipment. In order to achieve true "plug-and-play" interoperability, there must be a system in place to test equipment to the agreed upon standards and specifications to confirm compliance prior to operator procurement. Open RAN lends itself to creating an ecosystem of multiple vendors per disaggregated subsystem focused on their specialized strengths, which may otherwise not happen with a single monolithic vendor (e.g., create more individual RU, DU, CU

[4] *See* https://5gchallenge.ntia.gov/

vendors). This ultimately creates more vendor choices for operators as they customize their network deployment strategy to meet business and use cases. This presents a particular challenge to brownfield operators where an existing network system may not be built to accept new elements from a different vendor. Adoption of Open RAN by a brownfield operator may require more than replacing network equipment that is damaged or at end-of-life. As discussed below, operational support for multiple vendors in a RAN network requires an update to an operator's network deployment strategy as well.

Second, the vendor ecosystem will flourish when an industry-wide set of required baseline specifications and standards, referred to as a "profile," are developed. Currently, RAN interface standards and specifications produced by 3GPP and the O-RAN Alliance provided significant and meaningful optionality, which lead to a diverse set of implementations. Although each implementation conforms to the relevant interface standard or specification, those diverse implementations will not actually interoperate without a substantial system integration effort that is effectively custom development for each deployment. The development of one or more profiles will help create true plug-and-play interoperability.

By implementing an industry-agreed upon profile, new vendors can create network equipment and develop software to work across multiple network operators and use cases, which creates a better business case and incentives that will grow the number of vendors providing Open RAN technologies. This also contributes to scale, as small vendors normally excluded by network operators would gain access because they are able to meet the baseline specification and standards and perhaps create a lower cost option for operators. Having a separate conformance system in place that operators can rely on will also provide better access to operators for smaller and new entrant vendors. In addition, such a conformance system will help reduce the risk and enable adoption, particularly for smaller network operators that are unlikely to have the resources to test and ensure conformance on their own. This model is different than pre-certification of a group of components that follows the traditional RAN model and excludes new entrants. Instead, certification of discrete functional interfaces to a common "profile" will enable true plug-and-play interoperability.

The third, performance, is key to adoption by mobile network operators. Open RAN technologies must match, and eventually exceed, the performance levels, reliability, security, and features presented by traditional RAN elements today and must do all of this at a lower total cost. Such levels of sophistication in Open RAN equipment must be incentivized through a unified set of standards and specifications (a "profile") that match or exceed current performance levels. Without such guidance, vendors are spending R&D time on features that may not be of interest to or able to integrate with one or more mobile networks. As Open RAN matures and its 'open' capabilities equal and surpass the capability of monolithic vendors, this will create the opportunity of more flexible and customized performance and uninhibited innovation to meet operator needs.

Fourth, management is key to true interoperability. System management, including orchestration, in a multi-vendor environment requires tools and enablers to holistically manage

various network functions provided by different vendors. The underlying platform for management and operations must support different vendors based on open interfaces and open APIs. This is a dramatic shift away from today's proprietary systems that rely on one vendor making operations and management simpler. System management is critical to scaling Open RAN. As orchestration and similar open network management capabilities mature, scaling of multi-vendor Open RAN will become more efficient for operator deployment, operation, and performance activities.

Finally, investment is a significant challenge to the development, adoption, and deployment of Open RAN. Today, total cost of ownership (TCO) of a traditional RAN is lower than Open because single vendor deployments control cost by restricting access by other vendors to reduce system integration work – vertical integration. This creates a significant barrier to network operator investment in Open RAN. A second aspect of investment is influenced by large vendors with a vested interest in single vendor deployments. Large vendors invest significant resources and funds on research and development of traditional RAN systems that require operators to buy multiple components from a single large vendor. New, smaller vendors that are developing one or two Open RAN components do not have the funds or resources available for large R&D projects because the marketplace is not yet interested in components from smaller vendors. As discussed further below, investment to address the four challenges above is not readily available to all the vendors and operators that are interested in Open RAN. The Innovation Fund should prioritize funding new, small, and non-traditional vendors to drive competition and add diversity to the vendor ecosystem. Larger, established vendors have easier access to private investment and prioritizing funding of those larger, incumbent vendors will not further the stated goals of the Innovation Fund.

Questions 2, a, & b: Companies large and small, from operators to vendors, have publicly stated support and commitment to Open RAN technology, yet the ecosystem is slow in expanding.[5] CableLabs is aware that federal agencies, such as the Department of Defense, fund 5G related projects that may overlap with Open RAN technologies and contribute to the development of the ecosystem. However, these current funding opportunities may contain requirements and restrictions that historically impede the ability of small or non-traditional defense contractors to participate and are not necessarily focused on commercial applications (e.g., DoD's focus on military use of 5G). As a grant program, the Innovation Fund can be tailored to make funding available to smaller entities or those who are unable to comply with the long list of DFAR requirements tied to DoD funding. The Innovation Fund should focus on the commercial development and deployment of Open RAN technologies, unlike DoD funding that primarily targets the development of wireless networks and technologies for military use. Infusing funds into the Open RAN ecosystem will provide direct competition to the monolithic vendors if proper incentivized goals are set and managed. Operators will have to help drive this but will only start adopting (and driving) when Open RAN (1) is scalable, full featured,

[5] For instance, Vodafone is building Europe's first scaled commercial Open RAN network. *See* https://www.vodafone.com/news/technology/5g-open-ran-first-uk-site. Triangle, a small mobile network operator in the U.S. is replacing its equipment with Open RAN. *See* https://www.fiercewireless.com/tech/triangle-mavenir-tout-first-deployed-open-ran-network-fccs-rip-replace.

operationally reliable, (2) fits into their 5G and 6G infrastructure purchase cycles, and (3) fits into their virtualization/cloudification roadmap.

The Innovation Fund can also support entities with vast expertise in the area without the restrictions found in other government funding opportunities, while still protecting against waste, fraud, and abuse, and creating the potential for groundbreaking innovation.

From a standards perspective, a gap exists between the standards being developed and an agreement on how standards are implemented in technology development or incorporated into compliance testing and interoperability testing. We are currently unaware of funding, private or public, that supports standards development or implementation. As discussed throughout our comments, a critical goal for Open RAN should be common profiles to enable true "plug-and-play" deployment and the necessary test infrastructure to ensure that true "plug-and-play" interoperability is ongoing. The Innovation Fund can address these gaps by funding a variety of costs incurred by U.S. based organizations to participate in SDOs to contribute to the development of these common profiles; encouraging grantees to share the results of their work with SDOs and specification organizations to enable the specifications to mature; and fund participation of new and small vendors in testing activities.

Question 3: The need for change in network deployment strategies, operations, and management to successfully deploy Open RAN will lead to operators needing to build up and train dedicated workforces to assume new roles. Some of these roles in a traditional RAN system are currently staffed by those in IT operations. Across the United States the telecommunications workforce is under-resourced. Wired and wireless network providers are undergoing large scale build outs yet do not have the workforce necessary to accomplish this work in a timely manner. As virtualized networks are deployed, the workforce will need a different set of skills, more software engineers. Now is the time to build a workforce that is able to build, test, deploy, and maintain Open RAN and other virtualized network elements.

While section 9202(a)(1) of the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* does not specifically note workforce development as one of Congress' goals, NTIA could permit funding of projects that incorporate workforce development. Any funding for workforce development should require the demonstration of a direct connection to the advancement of the goals of the Innovation Fund, including the promotion and deployment of open, interoperable, and standards-based RANs. We also note that workforce development funding is available from many other federal agencies and the Innovation Fund is a finite resource. Thus, the NOFOs should not require a workforce development aspect nor use workforce development as evaluation criteria when reviewing grant applications.

Question 5: The telecommunications ecosystem, especially mobile networks, is very dependent on scale. We have seen tremendous vendor consolidation over the last 10 years due to this dynamic. With a strong dominance of a few vendors, the market for open and interoperable networks declines. This also impacts the development of standards and innovation, which historically are limited by the influence of the strongest players in the industry. Finally, a market with few dominant vendors leads to end-to-end network deals (i.e., vertical integration), further limiting the ability of new vendors to enter the market. All of these aspects lead to vendor lock-in, higher costs for network operators, stunted (or low incentive for) innovation, and potentially longer time to market for common or customized features.

In order to foster a healthier – more diverse and competitive – ecosystem, new vendors need to be supported, along with open and interoperable interfaces, so that operators can procure smaller parts of the network through different vendors. An important first step is the ability to procure equipment for trials or deployments to promote the advancement of Open RAN ecosystem and to validate and evaluate features, interfaces, and multi-vendor interoperability.

II. Technology Development and Standards

Question 6: In general, the end-to-end 5G stack would benefit from more innovation and additional funding. New vendors will need additional support in developing core, RAN, RIC, and BSS/OSS functions to compete in the larger mobile network ecosystem. The core network is critical to the mobile network and fewer vendors are chosen to provide this functionality to operators. The RAN network elements are also important and are typically the area where innovation drives success. Achieving open and interoperable interfaces between all elements of the 5G stack will be a benefit for the vendor ecosystem in the long term.

Research and development of open orchestration in various layers, e.g., open orchestration of core network functions, open orchestration of RAN components, and open orchestration of end-to-end systems would greatly accelerate the maturity of the Open RAN ecosystem. Additional funding for R&D of open interfaces, APIs, and use of AI/ML, specifically core network functions (e.g., user plane function), and the development of open interfaces and APIs to support O-RAN Alliance favored features such as edge computing and private networks would also contribute critical knowledge and concrete steps towards advancing Open RAN.

Questions 7, a, b, c: While the O-RAN Alliance is a mature industry alliance that developed specifications and 3GPP is a mature SDO that produced standards to enable market-ready Open RAN products, the optionality within the specifications and standards produced resulted in a barrier to vendors. There are many ways to show compliance with Open RAN standards and the structure of the standards allows each mobile carrier to choose a version of the standards for vendors that may not be chosen by a different mobile carrier.

To overcome this barrier in the standards environment, a common set of baseline Open RAN functional and performance requirements, including security requirements, (also referred to as a “profile”) that vendors can meet, and operators desire, where additional features and

requirements can be built as add-ons per individual operator needs must be established to enable scale and true plug-and-play interoperability.

To further encourage adoption and ease the process of deployment, a vendor interoperability test and certification program built on the baseline set of requirements (e.g., a profile) should be established. Following the model of the Wi-Fi Alliance and CableLabs' DOCSIS certification programs, these new Open RAN focused programs could provide compliance testing based on a set of standards required for every vendor and operator. Once those standards are verified, multi-vendor interoperability is confirmed, and operators can add additional features as desired. The creation of such a program is the best tool to ensure true interoperability and true Open RAN.

III. Integration, Interoperability, and Certification

Question 8: CableLabs suggests that the following projects could be funded by the Innovation Fund to help ensure 6G and future generation standards are built on a foundation of open and interoperable, standards-based RAN elements.

- Funding of a neutral organization or consortium to create the baseline requirements (a "profile") for Open RAN vendors. These baseline requirements would be used to establish the compliance-based interoperability needed to ensure plug-and-play capabilities and reduce the need for operator-specific System Integration.

- Initial funding to create Open RAN interoperability infrastructure necessary for certification programs.

- Funding for vendors to participate in the neutral organization and to pay for initial testing and certification.

- Funding to enable new and smaller Open RAN stakeholders to actively participate in the O-RAN Alliance and other relevant industry consortium and standards bodies.

- Funding to improve the stability and market readiness of Open RAN components through the creation of a field test facility where various Open RAN vendors can access normal and stress environments for compliance testing, performance testing, security testing, and problem solving.

Question 9: As mentioned above, the Innovation Fund can provide resources to establish a common set of baseline Open RAN requirements by a neutral organization and the development of a vendor interoperability test and certification program similar to the Wi-Fi Alliance and CableLabs DOCSIS certifications programs based on the baseline requirements. Projects funded by the Innovation Fund could support the adoption and deployment of open, interoperable, and standards-based equipment by contributing to the development

of the baseline requirements and participating in the interoperability test and certification program. The Innovation Fund could prioritize projects that commit to such work.

Interoperability testing and plugfests are effective in this space, but only if designed to test components in a true interoperable multi-vendor environment. Today, plugfests may be conducted between components from the same vendor that have been modified to satisfy a particular network operator. In addition, plugfests align vendors to do System Integration activities ahead of time, which does not advance the desire for true plug-and-play interoperability. While these events will test the vendor components, it would only be for the purposes of a unique network operator, not for the purpose of deploying open, interoperable, and standards-based equipment.

To enable such testing, additional steps such as establishing a common set of test cases shared across Open RAN testbeds and developing automation tools for continuous integration, deployment, and testing are important. Such steps can decrease time to market for functionalities and features of individual Open RAN sub-systems. Finally, testing and certification facilities and vendors should share learnings as contributions to Open RAN standards and specifications in relevant industry working groups.

Question 10: The most effective support for "integration of multi-vendor network environments" would be transitioning these multi-vendor deployments from System Integration based interoperability to compliance-based interoperability. This will take funding and efforts as described in the previous two answers.

An additional project appropriate for Innovation Fund funding is the creation of a field test facility where various Open RAN vendors can access normal and stress environments for compliance testing, performance testing, security testing, and compliance-based interoperability.

Questions 11 & 12: Historically, certification programs have accelerated adoption of specific technologies, a primary example of this is Wi-Fi certification. Operators and consumer electronics vendors do not need to do System Integration for every deployment or product that gets to market. Instead, operators and consumers can purchase any Wi-Fi certified equipment with the reassurance that it will provide a reliable and secure service. As described above, a similar approach would benefit the mobile industry by allowing more vendors to enter the marketplace, reduce operator costs, and accelerating deployment and innovation.

V. Trials, Pilots, Use Cases, and Market Development

Question 13: The full spectrum of potential 5G, 6G, and future generation use cases would benefit from open and interoperable, standards-based interfaces. Since Open RAN is not a new technology, but further radio access network interface specifications for open and interoperable multi-vendor network deployments, it would be applicable to both public and private 5G networks. As we have noted in other answers, given the very mature deployment

stage of 5G networks in the US and the world, greenfield and private networks might reap the most immediate benefit from these new interfaces and deployment options. However, over time, brownfield markets will benefit as well.

Recommended use cases should center around operator needs and include such topics as deployment strategy, network architecture, performance, reliability, stability, operations, optimization, and handover. With the adoption of O-RAN Alliance architectures and specifications, one group of new use cases that should be prioritized for funding are those that leverage the RIC (RAN Intelligent Controller). This includes real-time and near-real-time applications that help manage and orchestrate network usage.

Questions 14, 14a: Trials, feasibility studies, and proofs of concepts should center around operator needs and include such topics as deployment strategy, network architecture, performance, security, reliability, stability, operations, network optimization, handover, traffic steering, and resource sharing. Specifically, bringing new vendor solutions up to or past current vendor solutions in terms of features, performance, and security should be prioritized.

One specific consideration has been mentioned in other answers, the focus on developing the capability to do conformance-based interoperability. This would include development of interface profiles, test process and specifications, test environments, and live deployment trials to prove out multi-vendor performance and security. This would lower the risk and improve the confidence for to help operators move in the desired direction.

Testbeds that can support interoperability and end-to-end testing should be prioritized, preferably with emulators and actual 5G SA cores and UEs. This will support trials and pilots that promote multi-vendor interoperability as well as increasing performance, security, operations, reliability, and stability capabilities.

Question 15: Testbeds that can support interoperability and end-to-end testing should be prioritized for funding, preferably those testbeds with emulators and actual 5G SA cores and UEs. This will support trials and pilots in the near future that promote multi-vendor interoperability as well as increasing levels of complexity in performance, security, operations, reliability, and stability. Additionally, encouraging existing testbeds to collaborate, coordinate, and share knowledge and experience will help accelerate the ecosystem. These activities can be accomplished through the existing the O-RAN Alliance efforts or through a new entity created to help facilitate this discussion and exchange.

Question 16: Trials, feasibility studies, and proofs of concepts should center around operator needs and include such topics as deployment strategy, network architecture, performance, security, reliability, stability, operations, network optimization, handover, traffic steering,

resource sharing. Specifically, bringing new vendors solutions up to or past current vendor solutions in terms of features, performance, and security should be prioritized.

VI. Security

Questions 17, **a, b & 19**: Security is critical to the deployment, reliability, and successful performance of any network. The security of RAN systems is not simply determined based on the openness or closeness of the systems. Instead, at least three factors should be considered when evaluating the security of any system, including design security, implementation security, and deployment security.

First, security must be built in by design. The design of a RAN is primarily specified by 3GPP, with a small portion by other industry organizations such as the O-RAN Alliance. More specifically, the entire protocol stack of a RAN, including layer 1 (physical layer), layer 2 (Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), Service Data Adaptation Protocol (SDAP)), and layer 3 (Radio Resource Control (RRC)), are specified by 3GPP. The architecture of a disaggregated RAN, consisting of Central Unit (CU) and Distributed Unit (DU), is also specified by 3GPP, while further splitting of DU functions is specified by the O-RAN Alliance. Security of a RAN resides in the RRC layer for the control plane and the PDCP layer for the user plane, both of which are specified by 3GPP. The O-RAN Alliance is currently developing security specifications for the new fronthaul interfaces and functional entities largely based on the security specifications from 3GPP.

Therefore, from a design perspective, an Open RAN is of roughly equivalent security to a traditional RAN since the two versions share most of the security design based on 3GPP specifications. Security of the new interfaces and new functional entities introduced by the O-RAN Alliance are on track to be as secure as other parts of a RAN, since the corresponding security specifications are based on 3GPP specifications. There are some long standing security weaknesses in all RANs, such as a lack of protection of broadcast messages (e.g., System Information) and some unicast messages (e.g., RRC connection reject). However, those weaknesses are not unique to Open RAN, and should be addressed by 3GPP. This is the first area where the Innovation Fund can promote security in the development of Open RAN by funding participation by grantees in 3GPP and O-RAN Alliance to further support security work, by prioritizing projects that include the existing 3GPP and O-RAN security standards for Open RAN, and funding security related work to fill the security gaps across all RANs.

Second, security must be built into implementation during the development lifecycle of Open RAN products. This is a best practice for secure software development, albeit not standardized across the ecosystem. Under the best practice, security should be considered in each phase of the software development lifecycle.

To fully incorporate secure software development best practices, there are six recommended actions. First, Open RAN vendors and network operators will need to provide security training for project members on a regular basis, e.g., every year, so that project members understand

common security vulnerabilities, threats, and mitigations. The second phase is to perform threat modeling during the design phase, which identifies all software components and their interactions. This allows developers to identify threats against each asset and derive and implement the necessary security requirements and mitigations. The third phase is to perform security code analysis and review during the development phase to identify potential software vulnerabilities. This involves both manual review (e.g., for critical codes) and static and dynamic code analysis using automated tools. The fourth phase is to perform security testing, e.g., fuzzing and penetration testing, to identify hidden security vulnerabilities. The fifth phase looks at software development supply chains, access to build infrastructure, compiled binaries, signing keys for software updates, and true provenance for developed artifacts. The sixth phase is development of a security incident response process to handle reporting of security vulnerabilities after the product is released. The Innovation Fund can advance the adoption of the secure software development best practices by providing funding for projects to develop these resources within vendors and network operators.

Secure software development requires not only security expertise, but also security tools and additional resources to be successful. Large vendors have already invested in security and implemented secure software development into their product development and release cycle. For example, some large vendors have a centralized security group overseeing and assisting the secure software development in their product lines. Security groups may even have veto power over any product release. However, smaller vendors, such as some offering Open RAN products, may not have sufficient expertise and resources to fully adopt secure software development best practices. This is an area where traditional large RAN vendors may have some advantage over new entrants to the Open RAN market and the Innovation Fund can provide the necessary funding to overcome these resource barriers for new and smaller vendors.

The Innovation Fund is a unique opportunity for the government to make significant security expertise and resources available to Open RAN vendors to help them adopt and enhance their secure software development best practices. For example, the Innovation Fund can provide funding to a neutral organization that provides regular security training and meetings for the Open RAN community to educate developers, testers, and project managers working on Open RAN systems. Additionally, the Innovation Fund can encourage and provide resources to Open RAN vendors to adopt relevant security tools such as static and/or dynamic code analysis tools, secure code instrumentation tools, and penetration testing tools as part of a funded project. Innovation Fund resources devoted to research on future generations of new security tools will help both the Open RAN community and other industries.

Having addressed the design security and implementation security, the remaining primary concern is the secure deployment of Open RAN systems. To ensure 5G and future systems based on Open RAN are secured operationally, the Innovation Fund could require that the security features offered and supported by 3GPP and O-RAN Alliance specifications be used by all grantee vendors and network operators. For example, User Plane Integrity Protection (UPIP) should be enabled to protect the integrity of user plane traffic. New fronthaul interfaces

offered by the O-RAN Alliance should be secured, e.g., by using TLS or IPsec. Additional funding could be provided to standardize securing the cloud infrastructure on which Open RAN and 5G core are deployed.

As clarified by NTIA during the Listening Session, we understand that "security reporting" applies to security vulnerabilities identified by grantees during the course of work on an Innovation Fund project. As mentioned above, we support NTIA promoting the adoption of secure software development best practices by vendors and network operators by funding new or smaller vendors and operators to implement the processes necessary to identify and act on relevant vulnerability disclosures. However, due to the variety of projects and applicants likely to apply for Innovation Fund funding, security vulnerability reporting would not be a logical or relevant requirement for every project. For instance, projects focused on research and development of Open RAN components or interfaces could result in work that is not subject to security vulnerability reporting because the work is not performed on or intended for a live network available to consumers. Any such blanket requirement would impose a barrier on grantees and discourage applications for Innovation Fund funding. Thus, we do not support the addition of security vulnerability reporting as a grant program requirement, but we do support the grant program funding projects to help build the capability of small and new players to adopt secure software development best practices to process security vulnerability disclosures.

Question 18: Today, CableLabs is helping lead industry efforts in 3GPP and the O-RAN Alliance on security requirements, capabilities, and functions to be built into the Open RAN ecosystem. As the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council ("CSRIC") VIII notes: "The O-RAN Alliance's WG11 has performed a detailed threat analysis of O-RAN and continues to evolve O-RAN's security specifications to meet the security baseline expected by network operators and their users."[6] Ultimately, the implementation of security features and controls relies on vendors and network operators.

Question 20: The "zero-trust model" should be implemented in all RANs, traditional or Open RAN. While it is not currently required by 3GPP for traditional or Open RAN, the O-RAN Alliance WG11 is currently defining security standards based on the zero-trust model. The development of Open RAN presents an opportunity for quicker adoption of the zero-trust model. In particular, mutual authentication of each element and subsystem is key to a zero-trust architecture and development of the needed authentication mechanisms are a critical step in realizing the zero-trust model in Open RAN networks.

[6] CSRIC VIII Report on Challenges to the Development of ORAN Technology and Recommendations on How to Overcome Them at 17 citing O-RAN Alliance, O-RAN Security Threat Modeling and Remediation Analysis, O-RAN.SFG, O-RAN-Threat-Model-v03.00, March 2022.

VII. Program Execution and Monitoring

Question 21: CableLabs agrees that transparency and accountability are critical to the Innovation Fund's success. However, based on the statutory priorities detailed in section 9202(a)(1) of the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* there are a vast number of types of projects that could be funded by this program making it difficult to select metrics and data at this point in time. We note that asking applicants for measurable milestones, project specific schedules, and identifiable, measurable deliverables would be appropriate.

Question 22: Much of the day-to-day work in the Open RAN ecosystem is performed by newer and/or smaller vendors and network operators, and non-profit R&D organizations. NTIA should consider prioritizing awards to such organizations to build a diverse Open RAN ecosystem. NTIA can encourage these entities to apply by not adding barriers to eligibility or efficiency of the grant work, such as mandatory matching contributions, social impact criteria, workforce development criteria, burdensome reporting schedules, or mandatory partnerships.

Question 23: NTIA can permit, but should not require, teaming of applicants or the formation of new industry consortiums to be eligible for funding. Existing industry consortiums should be eligible entities for funding. Consortiums and partnerships should be required to propose a specific project with measurable outcomes to be eligible for funding. Decisions on specific projects to be funded should be made by NTIA and not delegated to a third party, in particular those that will not perform any actual work to further the statutory goals. Partnerships may allow the smaller and newer vendors to partake in the Innovation Fund by removing some of the barriers of grant administration. The existence of such arrangements should not be considered a priority or a preference in the evaluation criteria for a grant application.

Question 24: While NTIA can encourage matching contributions by grant applicants, NTIA should not require matching contributions, either monetary or in-kind, as such requirements present barriers to small businesses and non-profits. These are the exact entities interested in developing Open RAN technologies and the types of entities that lack the resources to invest in key priorities such as security. Large established vendors and operators may have the ability to provide matching contributions but may lack interest or incentive to promote the goals of Open RAN as stated in the NDAA and CHIPS Act.

If NTIA adopts a matching requirement or considers matching funds a priority or preference in grant criteria, NTIA should also clarify how matching contributions would be considered in line with the language from section 9202(a)(1)(D) of the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* that states: "[t]o the greatest extent practicable, the Secretary, acting through the NTIA Administrator, shall ensure that any research funded by a grant awarded under this paragraph avoids duplication of other Federal or private sector research."

VIII. Additional Questions

Question 27: We suggest that NTIA consider funding the following types of projects:

- Basic and advanced research on the Open RAN ecosystem.
- Development of Open RAN components and security features, not just promotion and deployment of security in the Open RAN ecosystem.
- Development of test plans and test infrastructure, and the subsequent testing of components and integration.
- Projects that cover parts of the network outside of the RAN. All RANs rely on wired and optical technologies to transport traffic in a secure and reliable manner; thus, funding should be available to improve the components of the wired network that support Open RAN and are necessary to promote the adoption of Open RAN.
- R&D of open interfaces and APIs for the core network, including edge computing, private network development, and open orchestration.

Question 28: CableLabs suggests that NTIA holds at least one additional webinar with a Q&A session after the RFC comments are filed and before the NOFOs are released to allow NTIA to ask questions or answer questions raised by the commenters that may influence the NOFO. This will also provide an opportunity for NTIA and participants to discuss information presented in the comments that may have varying views. There are additional topics not covered by this RFC that commenters may wish to raise, including grant evaluation criteria, period of performance, and certain statutory provisions.

Second, because this is a new grant program, applicants will appreciate the opportunity to ask questions during webinars once the NOFOs are released. If the NOFOs are distinct in the type of projects that may be funded, a webinar covering each NOFO may be warranted. An FAQ website covering the NOFOs and grant process would be helpful, including a mechanism to submit questions and receive answers in a timely manner before grant application deadlines.

IX. Additional Comments

As mentioned above, there are topics applicable to the Innovation Fund that were not directly raised by the questions in the RFC. CableLabs encourages NTIA to consider the following:

- Rolling deadlines for grant applications.
- Flexible periods of performance based on each project proposal.
- Clarification whether the $50 million cap is per project or grantee.
    - Based on the answer above, clarify if an applicant can submit more than one application and if only one application is to be submitted can proposals within the application be severed?
    - How will the $50 million cap apply to applicants that are part of multiple partnerships and applications?

- Clarification on the interpretation of section 9202(a)(1)(D) of the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* regarding matching funds and existing research efforts.
- Clarification that intellectual property rights for developed components, software, features, testing plans, and specifications should remain with the grantee.
    - We understand that the goal of the grant program is to accelerate the commercial market, not to create new technology for governmental use, thus the intellectual property rights should align with the eventual use of any intellectual property created under the grant program.
    - The preference is for grantees to retain simple ownership of intellectual property; however, clarification is needed whether intellectual property developed under the grant will be subject to Bayh-Dole.
    - We request clarification regarding additional restrictions or rules related to market and adoption such as FRAND, SEP, and other standards submissions.
- Clarification on whether grantees will be required to publicly share or disseminate project results, including at what point and to whom. To advance certain projects, coordination and information sharing with other grant recipients should be allowed, but not required. We remain supportive of the idea that grantees should share knowledge and experience to help accelerate the ecosystem through the existing the O-RAN Alliance or similar industry efforts or through a new entity created to help facilitate this discussion and exchange.

CONCLUSION

CableLabs shares NTIA and Congress' goals of promoting the adoption of open, interoperable, and standards-based networks. Our comments include recommendations for concrete actions NTIA can fund through the Innovation Fund and grant program rules to encourage a diverse set of projects and applicants.

As NTIA implements the Innovation Fund's statutory goals, CableLabs looks forward to contributing to the vision for security and true "plug-and-play" interoperability for open radio access networks.

Respectfully submitted,

/s Mark Walker
Mark Walker
Vice President, Technology Policy
CableLabs
m.walker@cablelabs.com

/s Jessica Almond
Jessica Almond
Director, Technology Policy
CableLabs
j.almond@cablelabs.com