Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, DC 20230

In the Matter of	)	
	)	
Public Wireless Supply Chain Innovation Fund	)	Docket No. 221202-0260
Implementation	)	RIN 0693-XC05
	)	

COMMENTS OF AT&T

AT&T appreciates the opportunity to comment regarding the Public Wireless Supply Chain Innovation Fund Implementation.

I. EXECUTIVE SUMMARY

The shift to Open Radio Access Networks ("Open RAN") has the potential to bolster U.S. leadership in wireless networking technology, a key component of nearly every modern infrastructure, security, and defense system under development today. Open RAN refers to a disaggregated approach to deploying mobile networks by using open and interoperable protocols and interfaces, which allows for increased flexibility over traditional RAN systems. The fundamental goal of Open RAN is to "open" the protocols and interfaces between the various subcomponents (radios, hardware, and software) in the RAN. Open RAN can be implemented with both vendor-neutral hardware and software-defined technology based on open interfaces and industry-developed standards. Traditional RAN, on the other hand, consists of radio, hardware and software and is proprietary, *i.e.,* "closed," which means there is minimal or no multivendor inter-operability.

Most, if not all, of the equipment comes from a single supplier. This makes it nearly impossible for operators to deploy a network using radios from one vendor with hardware and software from another vendor. Attempting to mix and match cell sites supported by different vendors typically leads to a performance reduction or an incompatible system. The result is even though most network operators strongly prefer vendor diversity and multivendor inter-operability in the RAN, the large-scale wireless networks deployed up until now are dominated by a single vendor in a geographic region. Not surprisingly, this has created vendor lock-in with high barriers to entry for innovators. These factors along with the need for scale have driven infrastructure industry consolidation leaving most U.S. operators with only a few primary options for RAN equipment. The status quo—namely that providers are dependent upon a limited number of primary vendors that are almost entirely based outside the U.S.—has increasingly been identified as national security matter for the United States.

For these reasons, in 2022 Congress created the Wireless Supply Chain Innovation Fund ("WIF") as part of the CHIPS and Science Act. The Wireless Innovation Fund provides an

opportunity to unleash innovation by speeding the industry transition towards more open, modular networks, thereby increasing the opportunity for vendor diversity, and reducing or eliminating vendor lock-in. While industry has already been driving in this direction through groups like the O-RAN ALLIANCE™, the U.S. government can leverage the WIF to make strategic investments, in partnership with industry, to shorten the time horizon and drive quicker adoption of Open RAN. This outcome would advance the competitiveness, economy, and global leadership of the United States with respect to 5G and NextG communications. U.S. government investment also sends a strong signal not only to the U.S. marketplace and investment community but also to our international partners who are making decisions today on how to secure their 5G supply chains.

While AT&T is fully supportive of the ongoing development of Open RAN, there remain challenges to widespread deployment in public wireless networks. National carriers serve a vast number of subscribers and a broad range of customer types, from consumers to enterprise to public safety. Our customers rely on our networks every day – one need look no further than the increased reliance on remote connectivity during the COVID-19 pandemic to understand the critical nature of our networks. Open RAN, while filled with promise, is not yet ready to take on this scale or diversity of needs. For these reasons, while AT&T continues to be a leader and strong advocate for Open RAN, deployment is going to take time and is dependent upon resolving a myriad of issues that is key for deployment at scale.

As such, our comments view Open RAN through the lens of how best to accelerate Open RAN for national operators such as AT&T. To be clear, there are promising deployments happening today, predominantly in enterprise 5G and greenfield environments, which have fewer challenges in terms of scale and ongoing feature support. However, more work needs to be done to bring these solutions to scale. These challenges fall into broad categories around the need for certification, better information around performance at scale, support for advanced features and capabilities, integration in brownfield environments, and cost.

We suggest a variety of actions NTIA can take to accelerate Open RAN development and deployment primarily by funding projects addressing key technical areas critical to the large-scale adoption of Open RAN. As discussed more fully below, these include, but are not limited to, areas such as open front haul, network management and analytics, virtual RAN, brownfield integration, network real-time intelligent control and service management orchestration, xApplications and multi-vendor network function integration. Perhaps most critical is the need to support integration efforts across all the domains associated with Open RAN including service management orchestration, real-time intelligent controllers, cloudification, open front haul and hardware integration. Each of these domains present their own challenges and should be considered as separate research areas in terms of grant eligibility.

There also is a need to improve both interoperability testing and integration to better develop the Open RAN ecosystem and avoid each carrier doing their own integration work. Formal certification can play a key role in ensuring that operators understand which equipment works well with others. The WIF can also be used to support increased U.S. participation and competitiveness in key standards bodies including 3GPP and the O-RAN ALLIANCE™ Finally, there are numerous Open RAN initiatives occurring around the world. NTIA can

leverage the fund to help convene industry and government to maximize the benefit of these disparate programs to drive the development of the greater Open RAN ecosystem.

In terms of the design of Notices of Funding Opportunities (NOFOs) there are a few key points. NTIA should establish broad eligibility for grants. NTIA should make efforts to ensure that the funds are widely distributed and not directed in large majority to single entities. A multitude of efforts should be undertaken to accelerate O-RAN. This should include projects proposed by large national carriers, smaller entities, large and small vendors, in all areas of the architectures – RU, CU and DU - and systems integrators. NTIA should also encourage teaming and industry consortiums to apply for grants. This will help avoid a duplication of efforts and ensure the funds are spread to their best utility covering a wide variety of areas vs. multiple projects driving at the same challenges. Further, developing a robust ecosystem and vibrant supply chain is going to require participation of both U.S. based and non-U.S. based entities. NTIA should consider grant requests which include participation from both U.S. based and non-U.S. based entities. Finally, NTIA, should be careful not to build excessive requirements into NOFOs setting too high of a bar for eligibility to encourage innovation.

Projects should largely take place in the U.S. but could be conducted in partnership with similar efforts conducted elsewhere to maximize investments in Open RAN and to avoid duplication of efforts. Establishing a venue for sharing information and experience between similar efforts in other countries could prove valuable. Finally, collaboration with like-minded governments is key. Achieving the necessary scale to drive the desired market outcomes will require adoption of Open RAN around the world. For this reason, ongoing, continued collaboration internationally is critical to success.

The remainder of our comments expand on these topics and address several of the areas raised by NTIA including: the state of the industry; challenges to O-RAN adoption; targeted projects to accelerate open RAN; the state of R&D; standards and O-RAN commercialization; integration, interoperability, and certification; trials, pilots, use cases and market development; and security.

II. BACKGROUND: STATE OF INDUSTRY

Open RAN is a continuation of trends towards "open" networks that have been occurring in the communications industry for years. As discussed in the National Security Telecommunications Advisory Council (NSTAC) Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem: 5G Appendix, "telecommunications operators traditionally built networks by interconnecting components that provide various network functions with standardized interfaces, including switches, routers, access nodes, multiplexors, and gateways."[1]

These network functions were implemented as integrated and closed systems – unique hardware tightly bundled with unique and inseparable software, along with a vendor-specific management and automation system. For operational ease, network operators traditionally would

[1] NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem (cisa.gov)

use one or two vendors for a given class of network components. Since most deployed network hardware components were infrequently replaced, vendor lock-in for both hardware and software emerged, with limited options for upgrading as technology advances.

Over the past decade, this paradigm has changed dramatically as network operators advanced in transformation from a hardware-centric model to software defined networks. In this new model, the hardware consists of standardized and commoditized hardware, which can be independently selected and upgraded to benefit from technology advances. The same hardware can support multiple network functions, which are implemented through software as virtual network functions running on commodity hardware. This software-based approach allows network operators to scale their networks to match demand, *i.e.*, the dynamic optimization of network resources.

These same developments are now expanding into the radio access network (RAN). The RAN portion of wireless networks contains wireless base stations which are connected to each other and to the Enhanced Packet Core or 5G Next Generation Core network. There are multiple components within each base station, most importantly the radio remote unit (at the antenna) and the baseband unit along with associated software. These components are typically connected by fiber and interoperate via a front haul interface, the Common Public Radio Interface (CPRI). In traditional wireless RAN deployments, vendors maintain key connections as proprietary/closed interfaces. For example, in the past a component from Company A (such as a radio) could not communicate with a component from Company B (such as a baseband unit), and individual base stations from one vendor would have limited interoperability with base stations from another vendor. This required network operators to build networks with fully integrated solutions from a single vendor or geographically separated from multiple vendors.

The O-RAN ALLIANCE™ is developing specifications to open and standardize these interfaces to move from dedicated proprietary hardware to commodity hardware. While 3GPP defines functional entities and a certain number of interfaces in the architecture, open RAN takes it even further. The benefits of this approach include increased network agility and flexibility, greater vendor diversity, increased innovation, and the potential for cost savings.

For its part, AT&T has played a key role in moving the industry towards open network architectures. AT&T is a founder of the Open Network Automation Platform (ONAP) which is part of Linux Foundation Networking (LFN) and an essential component of the 5G Super BluePrint (5G SBP) introduced by DARPA's Open, Programmable, Secure 5G (OPS-5G). AT&T also is a founding member of the O-RAN ALLIANCE™ whose mission is "to re-shape the RAN industry towards more intelligent, open, virtualized and fully interoperable mobile networks."[2] AT&T previously served on the boards of the Open Networking Foundation (ONF), the Open Infrastructure Foundation, and the Cloud Native Computing Foundation, and is a member of the Telecom Infra Project. AT&T is both a founding and full member of the NextG Alliance, where it chairs the NGA Founding Member Group and is one of the co-leads of the Steering Group. Finally, AT&T helped found and serves as chair of the Open RAN Policy Coalition (ORPC). Through the leadership of AT&T Labs, we also have decades of experience

[2] See O-RAN ALLIANCE e.V

in designing and operating lab environments to test and operationalize complex architectures that consist of multiple components as required in an Open RAN architecture.

As noted above, we fully support the long-term evolution towards Open RAN. In the next session, we will discuss the challenges to adoption.

III. CHALLENGES TO O-RAN ADOPTION

There are still major challenges with the Open RAN ecosystem as follows:

- **Interoperability**: Deployable open wireless networks require availability of interoperable components; however, large incumbent RAN vendors have shown some reluctance to accelerate development of O-RAN interoperability despite a significant push from the operator community. At the same time, even if vendors support 3GPP/O-RAN ALLIANCE™ standards, the challenges of deploying multi-vendor networks at scale are significant, especially for operators that have a significant embedded base of traditional RAN components. Nontrivial bilateral work between vendors, or among multiple vendors, is still needed that must be shepherded by a neutral party, typically the operator. No single operator can overcome the barriers delaying larger-scale Open RAN adoption and deployments, as each operator can only influence their own chosen group of vendors, and one operator's internal integration efforts may not be reusable by other operators even if the piece parts are all truly open and interchangeable. Grants directed towards establishing a means to support this integration on an ongoing basis, leveraging the experience from key operators, and combining resources to address the interoperability challenges outlined above would be beneficial to the entire ecosystem. This could include leveraging the WIF to fund the development of integration centers focused on interoperability testing and systems integration. Formal certification could also play a key role as discussed below.

- **Lack of Pre-certification**: Pre-certified combinations of piece parts, *e.g.,* RU, DU, CU, are not yet available. At present, there is no compelling financial incentive or support framework that would encourage vendors to collaborate with their competitors (rivals) to create such combinations. This is true for both new vendors and incumbents. This leads to high risk for operators who wish to deploy Open RAN, as they must make vendor selections on faith, and then drive one-off interoperability/integration efforts with chosen vendors at the operator's expense, often leading to significant budget overruns and time to market pressures (delays) that make traditional single-vendor solutions to appear less risky and less expensive even if that is not necessarily true in a long run.

- **Performance and Scalability**: Large carrier networks require equipment that can scale and support millions of subscribers. While we have seen some Open RAN deployments from entities such as Vodafone, Rakuten and DISH, among others, many of those have occurred in greenfield, rural or lower density areas. There is a need for data on the experiences of different operators in terms of performance at scale so operators can make informed decisions about the viability of Open RAN in macro wireless environments.

- **Support of advanced features/capabilities**: AT&T has a feature rich network that covers a full range of customer types with varying needs. Demonstrating how Open RAN equipment can fulfill those requirements is critical to large scale deployments. Support of advanced features such as massive MIMO, millimeter wave and network slicing are critical to deployment of Open RAN.

- **Equipment Cost**: Due to limited deployment /market for Open RAN, the equipment cost can be higher today. Part of this is because smaller Open RAN vendors cannot obtain the benefit of scale in acquiring components that comprise their equipment (*e.g.*, chips). This creates a catch-22 situation where greater competitiveness for Open RAN is dependent upon larger scale deployments decreasing cost, which in turn is only possible if the cost is lower or more competitive in the first instance.

- **Total Cost of Operations.** Also, the challenge of managing a multi-vendor environment can drive Total Cost of Operations (TCO) regardless of equipment cost. Large wireless operators need to be reasonably certain that Open RAN will drive reductions in TCO to support larger scale deployment. Some of this can only be gained through greater experience with Open RAN.

These challenges may be somewhat different for public vs. private networks. Private networks may not be required to operate at the same scale or with the same feature set as public wireless networks. It is also highly likely that different aspects of Open RAN may be gradually introduced into existing networks. This is already happening. For example, AT&T announced a deal in 2022 with Rakuten to use its site manager to quicken the workflow of wireless and wired networks. AT&T also recently announced an arrangement with Northrup Grumman and Fujitsu to test private 5G networks in support of the U.S. Department of Defense.

IV. TARGETED PROJECTS TO ACCELERATE OPEN RAN

The Wireless Innovation Fund can accelerate Open RAN including the following areas:

- **Open Front Haul and Integration Testing**. The development of Open Front Haul Interface between the RU-DU between primary suppliers and associated integration testing and certification. The O-RAN ALLIANCE™ has already defined Open Fronthaul specifications but there remains a need for integration testing and certifications which today rely mostly on individual operators working with vendors as outlined above. . Grants directed towards establishing a means to support this integration, such as formal integration centers and test beds, would benefit the entire ecosystem.

- **Network Management and Analytics**. The further development of the O-RAN Service Management and Orchestration (SMO) functionality. This introduces a foundation anchor point for disaggregation by allowing network elements that follow O-RAN specifications (O1 and O2) to directly integrate into the operator network by bypassing Element Management Systems and customer integration.

- **Virtual RAN**. VRAN enables hardware and software decoupling and introduces new hardware and platform vendors. System integration and cross-vendor operational automation is a key new challenge for this initiative as deployment of VRAN involves system engineering and tooling that works across the hardware, platform, and RAN vendors.

- **Accelerating O-RAN in Brownfield Networks**. Many operators already have an installed base of equipment that is closed and proprietary. The challenge is to find the right insertion point in the future more than trying to figure out how to convert 4G to be more open. Therefore, established vendors and operators with established networks are gradually moving towards Open RAN by working to seed the network with RU's that are software upgradable to the Open Fronthaul 7.2x specification (defined by O-RAN ALLIANCE™) and working with its vendors to begin opening more interfaces to achieve Open RAN by the insertion target date. NTIA can help foster brownfield deployment by sponsoring projects focused on interoperability between O-RAN ALLIANCE™ compliant equipment and legacy RAN technology already deployed at scale. This could include public disclosure of interoperability results of brownfield and greenfield settings and/or financial incentives for both operators and vendors to sustain interoperability testing and certification. Testing and certification is also required on an ongoing basis. Support for integration testing and incentives for participation will be an ongoing need for the Open RAN ecosystem.

- **Radio Intelligent Controller/Service Management Orchestration Integration**: Support integration testing of E2, O1, O2 interfaces to enable multi-vendor interoperability and support of xApps/rApps.

- **Multi-vendor network function integration**: As noted above, there is a need for continuous, ongoing network function integration between vendors. Most of this work is done by individual operators today working with their respective vendors. Grants directed towards establishing a means to support this integration on an ongoing basis, leveraging the experience from key operators, and combining resources to address the interoperability challenges outlined above would be beneficial to the entire ecosystem.

- **Life-cycle management.** Life cycle management between the different vendors is a challenge but is getting better with the release of interoperability and conformance specs that accelerate the move to open. Feature parity and performance parity (including scale, performance and security) are also key challenges to ensure the Open RAN community resolves to accelerate the transformation to openness.

- **Certification.** Additionally, there is a need to improve interoperability and integration testing along with certifications for equipment meeting the O-RAN ALLIANCE™ specifications. The journey to large-scale network integration of Open RAN components is a journey for all commercial operators. While there are certification programs emerging today, as we discussed further in our comments below, AT&T cannot move forward alone, and it would be highly valuable for all industry participants to be able to

learn from each other and rely upon certification to better understand which equipment works well with others.

- **International Collaboration.** There is also a need to enable greater collaboration internationally to advance Open RAN. For example, the U.K. is establishing a communications technology testing labs (see U.K. SONIC labs[3]). NTIA should support programs designed to facilitate combining efforts to avoid duplication. This could be done in partnership with entities like the Open RAN Policy Coalition and internationally focused entities such as the five eyes and quad forum.

V. STATE OF R&D, COMMERCIALIZATION AND STANDARDS

NTIA asks whether the state of Open RAN and 5G standards environment is sufficiently mature to produce stable, interoperable, cost effective, and market-ready RAN products. Maturity is relative. There are network operators today who are deploying O-RAN solutions to varying degrees. Deployment will depend on the operator and their individual requirements and comfort level with Open RAN. This will vary operator by operator and shouldn't be viewed as one size fits all.

In terms of specific standards or interfaces, the open front haul standard is the most mature (the 7.2x interface defined in the O-RAN ALLIANCE™ specifications). There are several other areas within the RAN that are ripe for further standards development which are largely aligned with the areas we highlight above. These include open front haul and integration testing, network management and analytics, virtual RAN, brownfield deployments, radio intelligent controller/service management orchestration integration, support of xApps/rApps, and multi-vendor network function integration.

Another challenge related to standards is related to workforce. The U.S. based Open RAN ecosystem requires a robust workforce that is trained in 5G/NextG technologies. The WIF can serve a role there by funding projects that will provide the opportunity for industry professionals to gain greater experience with Open RAN. This includes projects supporting integration which, as noted above, is a key challenge. The integration work between multiple vendors will require ongoing, continuous investment and engagement and can help drive the further development of a workforce to support Open RAN.

There also remain challenges to increasing the presence of U.S. or similar aligned companies in standards bodies. The NSTAC was tasked with drafting a Letter to the President[4] on how to increase U.S. competitiveness in relation to international standards and as part of that effort discussed this need to incentivize companies, including new entrants and smaller companies, to participate in the standards process. There are also challenges of hosting global standards meetings in the U.S. Streamlining the process and enabling more standards meetings in the U.S. would help advance O-RAN by making it more efficient for smaller players in the Open RAN space to attend meetings and participate.

[3] See SONIC Labs - Digital Catapult | Digital Catapult (digicatapult.org.uk)
[4] See NSTAC Letter to the President on Standards (cisa.gov)

Finally, regarding 6G, projects such as the ATIS Next G Alliance and the O-RAN ALLIANCE™ Next Generation Research group (nGRG) are doing the research necessary to drive the future standards toward an open and interoperable, standards-based RAN. This issue is also being addressed as part of "6G Emerging Technologies" interest group led by National Spectrum Consortium (NSC). We are in early phase of this discussion and current focus is to prioritize agenda items for inclusion in future 6G working groups. As 6G is an evolution to 5G technology, we expect open interfaces will be part of 6G working group discussion items.

VI. INTEGRATION, INTEROPERABILITY AND CERTIFICATION

Certification is an essential step to ensure multi-vendor network functions can inter-operate. This supports a successful marketplace and provides a level of assurance that products support the standards. However, each operator does additional testing beyond any certification/badging to verify compatibility with its own network. Certification and badging of O-RAN solutions represents a comprehensive mechanism ensuring confidence in the O-RAN solutions for both the operator as well as the vendor community.

The National Science Foundation PAWR Labs and the recently created North America Open Testing and Integration Center (OTIC) NYC Metro Area/East (COSMOS) are critical to validate compliance to standards and interoperability with other vendor hardware and should use the O-RAN ALLIANCE™ certification and badging program. O-RAN certificates state that an equipment or function is conformant to O-RAN specifications, whereas the O-RAN badges confirm interoperability or end-to-end functionality of an O-RAN solution. This will be critical to validate the compliance to standards and interoperability with vendor hardware.

Under this program, certification is applied on conformance tests, which involve only a single Device Under Test (DUT). This allows a transparent verification that the DUT behaves according to a concrete O-RAN technical specification. Badging is applied on interoperability tests (IOT) and end-to-end (E2E) tests. As the IOT and E2E tests involve multiple DUTs (from different vendors) the results may vary depending on the DUT combinations, deployment blueprints and test profiles. Conformance certification is defined as a verification of compliance of the Devices under Test (DUT) to O-RAN interface or reference design specifications, using O-RAN Conformance test specifications. Interoperability badging is defined as an assessment of interoperability of pairs of Devices under Test (DUT), which are implemented according to O-RAN interface specifications, using O-RAN Interoperability Test (IoT) specifications. E2E system integration badging is defined as an assessment of end-to-end system integration of groups of Devices under Test (DUT), which are implemented according to O-RAN interfaces, using O-RAN E2E test specifications.

The WIF could be used to establish an independent entity that coordinates this program among multiple OTICs and existing labs and resources in the U.S. establishing a more formalized certification program. Finally, there have been several plug fests around Open RAN. While plug fests are helpful the industry would also benefit from a more formalized certification regime. Plug fests have provided an excellent forum for vendors to perform interoperability testing to debug issues with implementation of standard interfaces and to identify gaps in standards. However, we now need to broaden the scope of interoperability and integration testing

through an independent national acceleration lab that can certify vendor equipment for compliance to Open RAN standards.

VII. TRIALS, PILOTS, USE CASES AND MARKET DEVELOPMENT

Making Open RAN a reality involves research and development that addresses not only the underlying technologies but also the comprehensive use cases that deal with the complexities of integration, compatibility, scalability and security. This requires continuous development, continuous testing, continuous integration, continuous deployment, and continuous monitoring throughout multi-year life cycles. This is sometimes referred to as a Development, Security and Operations (DevSecOps) approach to developing products, software or services. From an operator's perspective, the ultimate result of DevSecOps continuous improvement and continuous development are carrier grade components that are tested and engineered to meet or exceed "five nines" high availability standards, and that provide very fast fault recovery through redundancy (normally less than 50 milliseconds).

Due to nonexistence of Open RAN testbeds as of February 2018, when O-RAN was founded, up until today, we and other operators have met these challenges by working with, and building upon, our initial investments in the National Science Foundation (NSF) Platforms for Advanced Wireless Research (PAWR) program. The PAWR program has resulted in the creation of mobile and wireless research testbeds at several universities, including Rutgers University (COSMOS) and the University of Utah (POWDER), that are also designated by the FCC as Innovation Zones capable of wireless research in real world settings. Over the years, AT&T's work has helped to create a modern-day "guild" of significant wireless domain expertise with strong ties to relevant open-source communities and SDOs such as 3GPP, OpenAirInterface, srsRAN, O-RAN ALLIANCE™, ONAP, Kubernetes, OpenStack, ONF, and so on.

We propose that NTIA can leverage these existing test beds, combined with strong technical leadership from operators, to address a number of use cases, including but not limited to the following areas:

- Energy efficiency
- Context-based Dynamic Handover Management
- Context-Based Dynamic HO Management for V2X
- QoE Optimization
- Massive MIMO Beamforming Optimization
- RAN Sharing
- QoS Based Resource Optimization Network Slicing
- Traffic Steering
- Radio Resource Allocation for UAV Applications
- RAN Slice SLA Assurance
- Multi-vendor Slices
- NSSI Resource Allocation Optimization
- Local Indoor Positioning in RAN
- Massive MIMO SU/MU-MIMO Grouping Optimization

VIII. SECURITY

NTIA also asks about Open RAN security. AT&T agrees with conclusions from the Enduring Security Framework (ESF) paper on Open RAN Security Considerations: "security considerations always emerge in new open systems aiming for improved cost, performance, and supply chain benefits. Open RAN shares these security considerations too, and, with continuing efforts by the Open RAN ecosystem, they can be overcome."[5]

One of the common misconceptions about Open RAN is open interfaces introduce security risk. In fact, these open interfaces, defined in technical specifications, provide a foundation and architecture for improving security. Although operators procure and integrate open RAN network functions in new and different ways, we bring the same expertise, diligence, and requirements for security and resilience to these environments.

Throughout most of networking and computing history, security testing has largely been an independent activity separate and apart from the development life cycle. Not too long ago, security-focused quality assurance professionals performed testing as an afterthought. Today, however, DevSecOps includes security in every phase of the software development lifecycle. This approach ensures that security is built-in at every stage of the continuous improvement/concinuous development pipeline and is aligned with the best practices which are foundation in zero trust architectures. The philosophy behind DevSecOps is to begin security testing early in the development life cycle. DevSecOps integrates various security controls into the DevOps workflow, e.g., secure coding analysis using static application security testing (SAST), dynamic application security testing (DAST) as a black-box method, along with automated unit/functional/ integration testing. This enables developers to detect and remediate security issues in near real time rather than waiting until the end of the development life cycle.

The O-RAN architecture takes advantage of modern advancements in security automation and the trend in cloud computing towards "shift left." This ensures (1) that workloads running in the O-RAN network are validated securely (during build/deployment phase), and (2) that risk-based timely actions are taken when vulnerabilities are found before they are deployed in operators' networks. The federal government can motivate open source 5G network providers, e.g., operators, to implement O-RAN E2 service models (E2SMs) and related reference xApps by supporting our work in O-RAN from a policy perspective and funding perspective.

Security controls are not bolt-on capabilities but are integral to an operational open RAN. The Innovation Fund should make compliance with security specifications such as from the O-RAN ALLIANCE™ a component of multi-vendor test and interoperability of Open RAN solutions. Security controls based on industry standards, best practices, and frameworks are also necessary to fulfill the vision of interoperable, multi-vendor RAN powered by cloud services and software. All serve to help the open RAN ecosystem to build in security controls during development, deployment, and operations. The O-RAN ALLIANCE™ is a focal point for open RAN security standards, best practices, and frameworks to enable mobile network operators to

[5] https://www.cisa.gov/blog/2022/09/15/securing-5g-open-ran-architecture-cybersecurity-risks

operate an open RAN that meets and exceeds industry expectations for an open, interoperable, and secure system.

Many of the key areas for security controls are discussed in the ESF Open RAN Security Considerations[6] report and the FCC's Communications, Security, Reliability and Interoperability Council VIII Working Group 2 Report on the Challenges to the Development of O-RAN Technology[7]. Vendor equipment considered for grant requests should be capable of fulfilling the O-RAN ALLIANCE™ security specifications.

The Innovation Fund should also address challenging security issues in open fronthaul security. Open Fronthaul is built with an IT infrastructure but must perform like a real-time system. The Innovation Fund should consider projects addressing multiple Open Fronthaul security scenarios for consumer, enterprise, and military applications to meet the security objectives within the open fronthaul.

IX. PROGRAM EXECUTION

Finally, NTIA asks a series of questions about program execution including how to ensure a diverse array of stakeholders can compete for funding and the types of stakeholders NTIA should ensure are represented. In our estimate, NTIA should make efforts to ensure that the funds are widely distributed and not directed in large majority to single entities. A multitude of efforts should be undertaken to accelerate O-RAN. This should include projects proposed by large national carriers, smaller entities, large and small vendors, in all areas of the architectures – RU, CU and DU - and systems integrators.

NTIA should also encourage teaming and industry consortiums to apply for grants. This will help avoid a duplication of efforts and ensure the funds are spread to their best utility covering a wide variety of areas vs. multiple projects driving at the same challenges. Developing a robust ecosystem and vibrant supply chain is going to require participation of both U.S. based and non-U.S. based entities. It is also critical that the U.S. government have buy in from other governments to achieve the necessary scale. Given this, NTIA should consider grants from both categories mentioned above.

Projects should largely take place in the U.S. but could be conducted in partnership with similar efforts conducted elsewhere to ensure information sharing and to avoid duplication of efforts. As noted, above a venue for sharing information and experience between similar efforts in other countries could prove valuable. Finally, collaboration with like-minded governments is key. As noted, achieving the necessary scale to drive the desired market outcomes will require adoption of Open RAN around the world, not limited to the U.S. For this reason, ongoing, continued collaboration internationally is critical to success.

[6] See Open Radio Access Network Security Considerations (cisa.gov)
[7] See Communications Security, Reliability, and Interoperability Council VIII | Federal Communications Commission (fcc.gov)

X. CONCLUSION

AT&T understands that open architectures and open interfaces are the key to unlocking U.S. competition, innovation, and more comprehensive security principles. The innovation that O-RAN brings forward is based on the abandonment of traditional business models that promote vendor lock-in through proprietary solutions. As we have outlined in our comments, AT&T is well positioned to contribute to these efforts. We look forward to working with NTIA as the wireless innovation fund is implemented.