DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

5G Challenge Notice of Inquiry

Docket No. 210105-0001

COMMENTS OF AT&T SERVICES, INC.

February 10, 2021

AT&T Services, Inc., on behalf of itself and its affiliates (together, "AT&T"), respectfully submits these comments in response to the *Notice of Inquiry* (NOI) in the above-referenced proceeding. In the NOI, the Department of Commerce's (Department) National Telecommunications and Information Administration (NTIA), Institute for Telecommunications Sciences (ITS), under sponsorship of and in collaboration with the Department of Defense 5G Initiative, seeks comment "from all interested stakeholders to explore the creation of a 5G Challenge that would accelerate the development of the open 5G stack ecosystem in support of Department of Defense [(DOD)] missions."[1]

The NOI states "5G [is] a key modernization priority with the goal to advance U.S. and partner capabilities to fully leverage 5G technologies for military networking needs. A key innovation in 5G that is becoming more pervasive in the larger 5G ecosystem is the trend toward "open 5G" architectures that emphasize open interfaces in the network stack." [2]

The NOI then requests "comments and recommendations from stakeholders on how a Challenge to accelerate the development of the open 5G stack ecosystem in order to support DoD missions could be constructed in three broad categories: (1) challenge structure and goals; (2) incentives and scope; and (3) timeframe and infrastructure support."[3] The following are AT&T's comments on the concept of a challenge overall and in each of the areas mentioned in the NOI.

I. EXECUTIVE SUMMARY

There is an ongoing trend in communications towards open network architectures and away from proprietary closed interfaces, which have been commonplace in our industry for a number of years. This shift started early in the 2010's in the core of communications networks and is beginning to occur in the Radio Access Network (RAN). At the same time, there has been an ongoing consolidation of suppliers that has been particularly acute in the RAN. This has led to a rise in concerns about the long-term viability and competitiveness of supply chains (and the resulting impact on innovation) and the U.S.'s capacity to keep pace with international rivals.

[1] *5G Challenge Notice of Inquiry*, 86 Fed. Reg. 1949 (Jan. 11, 2021).
[2] *Id.*
[3] *Id.*

Against this backdrop, open networks have the potential to unleash more innovation by shifting the industry towards more open, modular networks. An analogy can be made to what occurred in the IT industry when, as interfaces were standardized, and opened, a wide range of companies providing IT infrastructure emerged. While industry is driving in this direction through groups like the O-RAN Alliance, we are at an inflection point where it is critical that government decisions appropriately set the stage for the future. In short, we need to make an investment in the future to ensure that the requisite scale and opportunities are available to expand the marketplace.

DOD can play a key role in making this future a reality. Congress recognized this in the National Defense Authorization Act (NDAA) for the Fiscal Year 2021 (FY21), in which it instructed DOD to carry out a "demonstration project to evaluate the maturity, performance and cost of covered technologies to provide additional options for providers of fifth-generation wireless network services."[4] The NDAA defines covered technologies as including "disaggregated or virtualized radio access network and core in which components can be provided by different vendors and interoperate through open protocols and interfaces, including those protocols and interfaces utilizing the Open Radio Access Network (commonly known as ''Open RAN'' or ''O-RAN) approach; and one or more massive multiple-input, multiple-output radio arrays."[5]

We believe that this Challenge can serve as a focal point, not only to fulfill the statutory requirements under the FY21 NDAA, but also to demonstrate the value of open network architectures. Such action can send 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. In particular, we suggest DOD, as part of the Challenge, establish a 5G test environment based upon an O-RAN reference architecture. DOD could establish a true plug and play environment open to any vendor that is compatible and with published, open interfaces to ensure interoperability between equipment. This would also extend to the software layer as we discuss in our comments. DOD can use this test environment to evaluate specific use cases for open networks including security, overall maturity, performance and interoperability. This test environment could extend to include both the physical interfaces between various components in the RAN to software. This will help DOD determine how to incorporate O-RAN into its 5G plans.

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 now part of the Linux Foundation and focuses on creating a "comprehensive platform for orchestration, management, and automation of network and edge computing services for network operators, cloud providers, and enterprises."[6] AT&T also is a founding member and chair of the O-RAN Alliance whose "mission is to re-shape the RAN industry towards more intelligent, open, virtualized and fully interoperable mobile networks".[7] AT&T also serves on the boards of the Open Networking Foundation (ONF), the Open Infrastructure Foundation, and the Cloud

[4] See NDAA FY2021 Section 225 p. 88
[5] *Id.*
[6] www.onap.org
[7] www.o-ran.org

Native Computing Foundation and is a member of the Telecom Infra Project. Moreover, AT&T has extensive experience in constructing lab environments, given the leadership of AT&T Labs, and in operationalizing complex architectures that consist of multiple components as would be required in an O-RAN configuration. AT&T looks forward to working with DOD to bring this vision to reality. The following are more detailed comments on the specific issues raised in the NOI.

II. INTRODUCTION

A. Industry Trend Towards Open Networks

At the outset, it is important to consider trends towards "open" networks that are already occurring in industry. An understanding of the various efforts underway will help identify areas where a challenge could be most effective in accelerating development.

The communications industry has been shifting towards more "open" network architectures for several 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,*[8] telecommunications operators traditionally built networks by interconnecting components that provide various network functions with standardized interfaces, including switches, routers, access nodes, multiplexors, and gateways. Most of 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 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."[9]

Over the past decade this paradigm has begun to change as network operators transform from a hardware centric model to software defined networks.[10] 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 and helps ensure maximum utilization of network resources.[11]

The move to a software-based construct requires disaggregation of the hardware and software and enables a high degree of operational automation. This migration started in our core

---

[8] *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem,* The President's National Security Telecommunications Advisory Council, (Sept. 3, 2019) at Appendix A: 5G Case Study.

[9] NSTAC report 5G Appendix at A-4.

[10] For example, AT&T has had an ongoing network transformation program underway for several years. See https://about.att.com/content/dam/snrdocs/7_Tenets_of_ATTs_Network_Transformation_White_Paper.pdf

[11] NSTAC report 5G Appendix at A-5.

networks. For example, in 2017, more than 50 of the largest network and cloud operators representing 70 percent of the world's mobile subscribers formed the ONAP project to deliver an open, standards-driven architecture and implementation platform. ONAP seeks to rapidly instantiate and automate new services and support complete lifecycle management of these software-based virtual network functions. As a result, operators can leverage their existing network investments while accelerating the development of a vibrant virtual network function ecosystem.[12]

While ONAP focused on core infrastructure, these same developments are now occurring in the radio access network (RAN) led by the O-RAN Alliance.[13] 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 are 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. Thus, while many operators use multiple RAN suppliers, the operators typically needed to build with single vendor's equipment in any given geographic area.[14]

The O-RAN Alliance is seeking to open and standardize these interfaces and move from dedicated proprietary hardware to commodity hardware. This will allow different vendors to provide radio units, baseband units, and backhaul, and for network operators to shift to modular networks with different components and software sourced from different suppliers. The result is much greater vendor diversity.

B. 5G Supply Chain and Open RAN

Another component that has factored into the aforementioned industry trends are the long-term implications for the wireless marketplace resulting from the consolidation of suppliers—particularly in the RAN where there are a limited number of suppliers.[15]

The combination of increased competition from China along with the consolidation of vendors has decreased vendor diversity and created challenges for new entrants. Upfront costs related to labor, equipment, and research and development all work to discourage new communications vendors from competing with established players.[16] However, the migration towards open networks may provide an opportunity to correct this by driving the industry toward

[12] See www.onap.org
[13] See www.o-ran.org
[14] *Id.*
[15] Comments of AT&T Services Inc. *National Strategy to Secure 5G Implementation Plan* docket No. 200521-0144 (AT&T Comments on 5G Implementation).
[16] *Id.*

a more interoperable, modular network design that will foster competition between suppliers and lower barriers to entry. It is critical that the U.S. put in place the right policy framework to allow the technical solutions championed by these groups to succeed. In effect a down payment on a more diverse supply chain in the future.

C. Open Networks and Security

Open network architectures can also benefit security. Open architectures allow the operator to fully control the security of the network, ultimately enhancing the operational security of their network. One benefit is greater visibility to security events: A network operator will have direct access to more data about network performance because the components are disaggregated and connected through open interfaces. This will allow them to gain more security insights about potential security problems earlier. Data will be finer-grained and represent activities between network functions that were previously hidden by internal vendor interfaces. Further, data about the running state of network functions will be more easily available through open management interfaces. This data can be combined with security log data to drive root cause analysis.

Another security benefit is that operators can shift the security capabilities closer to the edge of the network and stop attacks closer to the source. The introduction of open interfaces in the RAN allows the operator to distribute security analytics throughout the network and move RAN monitoring to the edge. This creates opportunities to create edge-focused analytics that speed the detection of network attacks and drive closed-loop actions at the RAN which blocks malicious traffic from reaching the Core. Rapid detection and response enables efficient and more secure support of mobility services, especially IoT services by more effectively preventing DDoS attacks on the RAN by rogue mobile devices. Distributed security analytics allows an operator to share insights between the RAN and core, as well as between different RAN locations. Such insights can be used to take measures to protect radio units adjacent to a unit under attack, or to use insights about the core to protect potentially vulnerable RAN units.

Open networks will also allow operators to integrate best in class security platforms with open interfaces defined to be secured using modern, industry standard security protocols. Since security platform vendors typically provide native support for standard protocols and interfaces, the operator can integrate new security platforms without implementing custom adaptors for vendor proprietary protocols and interfaces. Furthermore, network function vendors will deliver regular protocol updates to stay current with the protocol releases, allowing operators to stay current with industry best practices at no extra cost.

Finally, open networks can speed the complete automation of network management. Automation enables zero-touch management which eliminates the security risks inherent in human access to network functions (NF). Such risks include the threat of humans accidentally altering the security posture of a network function or maliciously harvesting credentials, changing configurations, or implanting malware within the network. Automation also increases closed loop response to changes in the network. For example, by using an open management interface for checking the security posture of a network function, the operator can quickly detect and fix degraded configurations through closed loop management. Open networks will also

increase the speed with which operators can install software and operating system security patches, thus enabling the operator to minimize the amount of time a vulnerability is in the network.

D. Role of DOD

Both NTIA and DOD can play a key role by championing the technology within government. As we highlighted in our comments to NTIA on the *National Strategy to Secure 5G Implementation Plan*, the U.S. government can play a key role in supporting the development of open and interoperable wireless networks, collaborating with industry to facilitate the development of global 5G standards and open-source software, promoting research and development of open technologies and supporting vendor diversity and "open" platforms worldwide outside the U.S.[17]

In particular, DOD can use the Challenge a test environment, either in a testbed or small-scale deployment, to demonstrate how an O-RAN Alliance compatible architecture is deployed and at the same time fulfill DOD's mission requirements. Such an environment should be predicated on the use of open RAN compatible equipment, including ensuring equipment is not only open RAN compatible but also has published specifications on their interfaces to ensure an open environment where all vendors can plug-and-play in this space. This should also include open interfaces to the applications that would run over such a platform to ensure that if an operator used controllers from different vendors, that software would not have to be revised or rewritten to accommodate different suppliers thereby ensuring the greatest level of compatibility and openness. Such an environment can also serve a key role in addressing critical issues to the success of open RAN including network security, completeness and maturity.

In this context, the following are our responses to specific questions raised in the NOI.[18]

III. CHALLENGE STRUCTURE & GOALS

A. How could a Challenge be structured such that it would take advantage of DOD's role as an early U.S. Government adopter of 5G technology to mature the open 5G stack ecosystem faster, encourage more participation in open 5G stack development including encouraging new participants, and identify any roadblocks to broader participation?

More important than the specific mechanics of how the challenge is structured is to ensure that a Challenge is based on O-RAN Alliance specifications or otherwise open interfaces to ensure that equipment is truly interoperable. This should expand beyond not only the hardware interfaces, such as those between the radio, baseband or hardware and software, but also to ensure that software can be written across multiple vendors' controllers. Ensuring true interoperability means that applications will not stand as an impediment to changing out equipment or moving to a more modular design. The specifications also should be published, open and non-proprietary. There are many examples today of different vendors interoperating

[17] *Id.*
[18] *Id.* at *10-13*

but in many of those instances the specification is proprietary. A key role for DOD could be to build a base platform compatible with the O-RAN Alliance specifications and allow for anyone to participate. The key interfaces to test for interoperability and openness include the open front haul interface between the Radio Unit and the Distributed Unit (RU/DU) or what is commonly referred to as an CPRI or eCPRI interface. It is also important to ensure open APIs in the mid haul interface between the CU/DU and software that may be resident on the platform. In terms of the mechanics of the Challenge, it could be modeled after the numerous previous challenges DOD has performed such as the Spectrum Collaboration Challenge (SC2) hosted by DARPA.[19]

B. How could a Challenge be structured to focus on the greatest impediments to the maturation of end-to-end open 5G stack development?

A Challenge should focus largely on the Radio Access Network (RAN) and associated software. As noted above, there is a need for software that is compatible between multiple vendors controllers. The O-RAN Alliance has formed the O-RAN Software Community which is "a collaboration between the O-RAN Alliance and Linux Foundation with the mission to support the creation of software for the Radio Access Network."[20] A DOD Challenge could be constructed to focus on both of these areas. The DOD could also examine how these software solutions can be tailored to meet DOD's mission requirements.

C. What should be the goals of a Challenge focusing on maturation of the open 5G stack ecosystem? How could such a Challenge be structured to allow for the greatest levels of innovation? What metrics should be used in the assessment of proposals to ensure the best proposals are selected?

As noted above we believe a Challenge should be focused on incentivizing the maturation of open RAN and open RAN related software. There are a variety of metrics that could be used to measure success. For example, if DOD were to create a test environment, some gauges might be: How much equipment is successfully implemented? What are the impacts on network performance or latency? How can we validate that the equipment has properly mitigated security threats? Another critical metric is a measure of the "openness" ecosystem. Quantifying the degree to which participants program O-RAN attributes into their solutions is essential.

For security, DOD could engage with the National Institute of Standards and Technology (NIST), which recently established a 5G security test bed. This would be a means to partner with NIST and industry on the development of zero trust architectures for open networks, to measure or test interoperability or a traffic simulator to measure performance and traffic dynamics. NIST is presently building its test lab at the National Cybersecurity Center of Excellence (NCCOE) and DOD can gain synergies by partnering with NIST. AT&T is a founding partner and key contributor to this initiative.

D. How will the open 5G stack market benefit from such a Challenge? How could a Challenge be structured to provide dual benefit to both the Government and the open

[19] https://archive.darpa.mil/sc2/wp-content/uploads/2019/02/SC2-Rules-Document-V3.pdf
[20] https://www.o-ran.org/software

5G stack market?

In our view, DOD can play a vital role in demonstrating the viability of open RAN. We are at a critical global inflection point where countries are developing their national 5G and beyond strategies and many are considering to what extent they will allow certain untrusted vendors into their marketplace. Open RAN focuses less on specific suppliers and more on openness, and if the U.S. Government can demonstrate successful open ecosystem trials and architecture, that may provide the confidence for other nations to more aggressively support open RAN. In this context, DOD and broader U.S. government support is effectively a down payment to increase the prospects for open RAN over the long term while the technology is taken to scale.

This nascent shift in network architecture presents a particularly important opportunity for the United States, which has typically led the world in developing innovative software-based applications. With its planned engagement, DOD can help set a common target or objective to strive for and leverage its procurement capabilities to drive the private sector towards open RAN compatible architectures. DOD's involvement can also help establish expectations and normalize a service delivery architecture across the market, as well as help address perceived security concerns around open architectures.

IV. INCENTIVES & SCOPE

A. *What are the incentives in open 5G stack ecosystem development that would maximize cooperation and collaboration, promote interoperability amongst varied open 5G stack components developed by different participants, and mature desired featured sets faster with greater stability*?

DOD can leverage its procurement capabilities to provide a major incentive for the use of open RAN compliant equipment, software and applications. If DOD develops a reference architecture based upon O-RAN Alliance specifications and uses that architecture in certain DOD procurements that may fit the criteria for an open RAN application, DOD will drive suppliers to support open interfaces. Doing so is consistent with long-established preferences for a competitive environment for government[21] with the caveat that an open RAN architecture may not be appropriate in <u>all</u> instances, DOD will have to determine when and where and for what use cases it may be most appropriate. DOD can use the proposed test bed or environment to ensure that open interfaces are readily available and can scale to meet demand and performance expectations for DOD missions.

Congress also included the Using Strategic Allied (USA) Telecommunications Act in the NDAA FY2021 legislation. The legislation would establish a Public Wireless Innovation Fund to be administered by NTIA in consultation with NIST, DHS, DARPA, and the Director of the Intelligence Advanced Research Projects Activity of the Office of the Director of National Intelligence to set up a grant program to support the development and commercial application of, among other things, accelerating the development of open interface standards-based compatible, interoperable equipment set forth by organizations such as O-RAN. There may be an opportunity to structure the challenge to partially take advantage of this program.

[21] AT&T Comments on 5G Implementation at 4.

B. *Could a Challenge be designed that addresses the issues raised in previous questions and also includes test and evaluation of the security of the components*?

As noted above, a clear benefit of such a challenge could be to demonstrate how to deploy open networks in a secure fashion. There are a variety of ways this can be done employing concepts like zero trust[22] networking in which it is assumed that an attacker is present in the environment, each network function is protected against attacks and breaches, and the network can be deployed with security controls that limit internal lateral movement. An open network lends itself to the implementation of a zero-trust architecture that enforces a consistent security posture for all network functions because security will be defined as part of each open interface. Security will be enabled on each component of a network as it is deployed. For example, authenticity, integrity, and confidentiality will be enabled on each open interface and the runtime credentials will be provisioned automatically. Similarly, each component will be configured in a hardened state, and log collection enabled. Security will not depend on a trust relationship between components from a single vendor that interact via proprietary interfaces. Furthermore, as new technologies develop, new controls that enhance zero trust principles can be uniformly added to the network.

C. *Could a Challenge be designed that would require participants to leverage software bill of materials design principles in the development of components for an open 5G stack*?

Software transparency is a critical security issue as demonstrated by the recent SolarWinds hack. A software bill of materials is critical, particularly in an open-source environment, in understanding what libraries are being reused in code. Software bill of materials design principles could be incorporated as part of a broader security component to the challenge. Open-source security concerns can be lessened by using a software bill of materials for each network function to make the operator aware of all open-source vulnerabilities associated with it. This will enable the operator to protect itself from existing open-source vulnerabilities, as well as to encourage their suppliers to provide timely fixes in the form of software upgrades. Operators can use the knowledge about open-source vulnerabilities to develop security test suites that actively test the impact of known vulnerabilities on the security posture of the network. Finally, operators can improve the security of open-source software by actively improving the quality of open-source code produced by strategic communities such as ONAP and the O-RAN Alliance.

D. *Many open 5G stack organizations have developed partial implementations for different aspects of an open 5G stack. What portions of the open 5G stack has your organization successfully developed with working code? What portions of the open 5G stack does your organization believe can be developed quickly (6 months or less)? What development support would best enable test and evaluation of the different elements of an open 5G stack*?

[22] Zero Trust Architecture. NIST Special Publication 800-207. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

AT&T is committed to deploying an open network. AT&T has developed and collaborated on varying aspects of an open 5G stack, including the following:[23]

- AT&T and CommScope are showcasing O-RAN's Vendor Agnostic Operations, Administration and Maintenance (OAM) Architecture and O1 Interface Specification.
- AT&T and Nokia have co-developed an open source Near-Real-Time Intelligent Controller (near-RIC) in O-RAN OSC running at the Network Edge on an Akraino-Based Open Cloud Platform.
- Ciena, Radisys, Wind River, AT&T and DISH Network are co-sponsoring a demonstration of 5G Edge orchestration and optimization.
- AT&T, Commscope, and Intel are demonstrating mmWave 5G gNB and 7.2x open fronthaul demo.

In 2021, AT&T will be conducting a number of trials with vendors and partners to validate, test, and mature the O-RAN software stack for both 5G and 4G/LTE, and will continue working to accelerate innovation of third-party network applications.

AT&T has also been a key player in the Linux Foundation ONAP Project, leading the charge to provide automation capabilities in support of SDN/5G and ORAN as follows:

- Instantiation of 5GC CNFs on Open source k8s cluster using ONAP (5GCFree) – Open 5G Stack.
- Discussion with DARPA to position ONAP as part of Open, Programmable, Secure 5G Network - https://www.darpa.mil/program/open-programmable-secure-5g.
- Development and verification of a number of 5G use cases and functional requirements using ONAP, including E2E Network Slicing, 5G SON (Self-Organizing Networks), and 5G Network optimization.
- Some components of ONAP are also re-used in XGVela, a 5G cloud-native open-source framework.

AT&T further collaborated with Intel to create the Airship opensource project, hosted by the Open Infrastructure Foundation. Airship is a collection of loosely coupled but interoperable open source tools that declaratively automate cloud provisioning. Airship is a robust delivery mechanism for organizations who want to embrace containers as the new unit of infrastructure delivery at scale. Starting from raw bare metal infrastructure, Airship manages the full lifecycle of data center infrastructure to deliver a production-grade Kubernetes cluster with Helm deployed artifacts, including OpenStack-Helm. Airship allows operators to manage their infrastructure deployments and lifecycle through the declarative YAML documents that describe an Airship environment. AT&T uses Airship and other CNCF opensource projects like Kubernettes to build and deploy the 5G user plane and control plane.

[23] *O-RAN Alliance Continues to Grow as Global Operators and Suppliers Reach Across Borders to Collaborate on Open Innovation in Radio Access Networks*, available at 2020-02-20_O-RAN+progress+PR_v1.0.pdf (squarespace.com).

On the topic of development support, the Challenge would benefit from an Open 5G Cloud infrastructure that serves as the network function virtualization infrastructure (NFVI) for the test and evaluation of the different elements of an open 5G stack, including the Open 5G Cloud stacks. AT&T encourages DOD/NTIA and DOD to stand up a 5G cloud infrastructure based on the newly formed Linux Foundation Project called Anuket. Anuket provides benefits to mobile network operators (e.g., telecommunication companies, enterprises, and others telcos and enterprise operators) with a common NFVI for testing open 5G workloads based on NFV and CNF. Anuket "delivers a common model, standardized reference infrastructure specifications, and conformance and performance frameworks for virtualized and containerized network functions, enabling faster, more robust onboarding into production, reducing costs and accelerating communications digital transformations."[24]

E. *What 5G enabling features should be highlighted in the Challenge, such as software defined networking, network slicing, network function virtualization, radio access network intelligent controller, radio access network virtualization*?

NTIA and DOD would benefit from a focus on all 5G enabling features listed: software defined networking, network slicing, network function virtualization, radio access network intelligent controller, and radio access network virtualization. An expanded list of 5G enabling features for consideration are millimeter wave; massive MIMO; network ultra-densification; new radio access techniques; multi-access edge computing for 5G core and RAN functions; network edge computing where cloud service providers and enterprises interwork with the 5G core; mission critical services applicable to FirstNet and DOD needs including device-to-device connectivity; scalable Internet of Things; big data and mobile cloud computing; and ONAP for the management and orchestration of a diverse and open 5G network.

An underlying, key enabling feature of an Open 5G stack is the 5G cloud infrastructure. As noted above, all Challenge activities would benefit from a common 5G cloud infrastructure based on the Linux Foundation Anuket Project because it would minimize the level of customized support, improve interoperability, and reduce cost, all benefiting 5G network operators (telcos, enterprises, etc.), cloud infrastructure vendors, and network function vendors.

To round out a key list of 5G enabling features, the NTIA and DOD would benefit the challenge with strong 3GPP security mechanisms for open 5G networks, including Security Edge Protection Proxy (SEPP) for 5G roaming and Network-to-Network Protection, Increased Home Network Control for Authentication, and Unified Authentication Framework.

V. TIMEFRAME & INFRASTRUCTURE

A. *What software and hardware infrastructure will be needed to successfully execute this Challenge*?

[24] https://anuket.io/

DOD could model a test bed after the NIST NCCOE security test bed mentioned above. As for specific requirements, once DOD has more specific requirements, AT&T Labs has extensive experience with integrating network technologies and has multiple labs and looks forward to opportunities to partner with DOD on implementing their vision.

B. What is a reasonable timeframe to structure such a Challenge? Should there be different phases for such a Challenge? If so, what are appropriate timelines for each suggested phase?

We believe that DOD should establish an iterative process that runs over a number of years. It is a reasonable objective to assume that if DOD proceeds on establishing a test environment that it could be turned up within 6-12 months and initial equipment could be tested or evaluated. Additional use cases could be tested over time. The goal should be start small, develop an iterative process and layer on more complex capabilities over a number of years.

VI. APPENDIX: PROPOSED USE CASES FOR POSSIBLE TEST ENVIRONMENT

As noted above, one way DOD can construct a challenge is through the creation of a 5G test environment or smaller scale deployment based upon an O-RAN Alliance compliant architecture. DOD could establish a true plug-and-play environment open to any vendor that meets the O-RAN Alliance specifications and has published interfaces to ensure interoperability between equipment. This would also extend to the software layer as we discuss in our comments. The DOD could also conduct specific use cases or test scenarios around demonstration security for open networks such as those outlined below.

Security Use Case 1: Software Bill of Materials (SBOM) based testing.

The open 5G ecosystem will be increasingly dependent on software that includes open-source code. Open-source use in communications networks has received increasing scrutiny because the exploit of a known open-source vulnerability in a 5G network could be devastating. To reduce this risk, this proposal will develop a prototype SBOM based testing platform consisting of a suite of tests for known vulnerabilities (CVEs) in open-source packages commonly used in 5G component implementations and a methodology for integrating the CVE tests into end to end (E2E) tests of an application.

Security Use Case 2: Testing race condition between xAPPs in the O-RAN Alliance RIC.

Ericsson and others have identified competing xApps as a potential threat to the security and availability of an open RAN deployment.[25] [26] As more xApps are introduced into the RAN to provide near-real time management of network functions, the chances arise that different xApps will introduce race conditions. This proposal will develop a model driven testing platform

[25] *Security considerations of Open RAN*, https://www.ericsson.com/en/security/security-considerations-of-open-ran?utm_source=linkedin&utm_medium=social_organic&utm_campaign=Networks_MANA_Radio_System-Antenna_System_20200819.

[26] The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components. https://www.o-ran.org/blog/2020/10/24/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components.

to validate that a set of xApps operate independently, without causing race conditions or other anomalous behaviors that could compromise the security of the RAN.

Security Use Case 3: 5G Slicing Security Honeypots.

A Honeypot is used to create a virtual trap to lure attackers to study their techniques so as to improve the security of the network. This use case will build prototype 5G-native honeypots using 5G slicing. When malicious traffic is detected, a honeypot slice will be created automatically, and the malicious traffic will be transported on the honeypot slice. The normal traffic will continue to be carried as normal. The malicious traffic will be collected and used in training AI/ML-based security analytics.

Security Use Case 4: Enhancement of 5G Zero Trust Architectures.

Zero trust focuses on the goal of preventing unauthorized access to data, services and resources coupled with making access control enforcement as granular as possible. The use case will focus on collecting data that can be used to better train an access control model to restrict access to the user plane and to the management plane. The use case will focus on IoT device access to the user plane because of the threat posed to the network by such compromised devices.