5G Prize Challenge Notice of Inquiry Analysis

On January 11, 2021, the National Telecommunications and Information Administration (NTIA) issued a 5G Challenge Notice of Inquiry (NOI) on behalf of the Department of Defense (DoD). On February 16, 2021, NTIA received 51 responses, totaling 384 pages. The NOI requested information on how to use Prize Challenges to accelerate the development of the open 5G ecosystem and support DoD missions. The NOI questions were intentionally broad to illicit widescale response and to ensure technical neutrality.

This document provides an analysis of the NOI responses. This analysis was created by NTIA's Institute for Telecommunication Sciences (ITS) to inform future collaborations between the DoD and NTIA. This analysis is anticipated to inform the creation of a 5G Challenge, with the goal of accelerating the maturity of 5G open interfaces, promoting interoperability among vendor modules, and lowering barriers of entry into the 5G marketplace.

In the NOI responses, respondents directed recommendations to the DoD, NTIA, and/or the creators of the 5G challenge. Throughout this document, we refer to these entities collectively as the "challenge team." The recommendations and opinions in this document do not represent those of DoD, NTIA, or the challenge team.

The remainder of this document is organized as follows. "High Level Themes" on page 2 describes general trends. "Enable Vendor Diversity of Commerce" on page 5 describes tools and capabilities that would enable improved vendor diversity. "Security" appears on page 8. "Prize Challenges" on page 9 contains advice on how to structure prize challenges. "NOI Response Summary" on page 13 provides a table that briefly describes each NOI response.

High Level Themes

The NOI responses contain a wealth of information from standards organizations, equipment manufacturers, mobile network operators, advocacy groups, federal agencies, universities, etc. Like the parable of the blind men and the elephant, each NOI response contains unique insights on some topics and omits other topics. This section focuses on three overlapping, high level themes that emerged from the comments. The first two topics are unprompted by the NOI questions, which may emphasize their importance.

Support Existing 5G Endeavors

Respondents encourage cooperation with existing efforts, particularly 3GPP (3rd Generation Partnership Project), the O-RAN (Open Radio Access Network) Alliance, the Telecom Infra Project (TIP), OpenAirInterface Software Alliance (OSA), National Spectrum Consortium (NSC), and Open Networking Foundation (ONF).

Respondents express concern that DoD will create their own standard or support one vendor's variant.

"DoD efforts, outside existing structures, could be counterproductive, draining resources from an effort already underway." T-Mobile

Clarify Definition and Scope of "Openness"

The NOI used ambiguous language to avoid bias ("open 5G stack ecosystem"). However, many respondents note the need to clearly define what is meant by "openness." The following types of openness were mentioned by respondents:

- Open interfaces
- Open-source
- Open architectures

Open interfaces are strongly supported in most NOI responses. However, there is concern that requiring all components to have open interfaces may be impractical in the near term. Respondents encourage focusing on open interfaces for specific components instead of addressing all interfaces simultaneously, and recommend assessing existing interfaces and frameworks while designing the 5G Challenge.

"While an Open 5G ecosystem is a welcome sign, not all 5G ecosystem layers may be mature enough to meet the requirements." VMware

Respondents did not strongly advocate for open-source solutions and in some cases opposed them, although support exists from academia and organizations who distribute or support open-source (e.g., Linux Foundation). Comments in opposition identified industry's need to retain intellectual property (IP) rights, and the need to maintain competitive advantage, as two barriers to open-source adoption.

"...the commercial world has decomposed the logical elements and interfaces as much as necessary to support new commercial deployment models but the DoD will require further decomposition ... for 5G-derived technologies to operate in highly contested RF and cyber environments..." Lockheed Martin

The NOI responses did support open-source solutions for infrastructure support tools and for infrastructure solutions, including open-source hardware, mobile edge platform software, and orchestration software that manages mobile edge computing. The respondents conclude that the 5G Challenge is an opportunity to close security gaps in open-source solutions.

Support for open architectures was implied by a more commonly expressed support for "softwarization."

Potential Benefits to 5G Open Architecture Deployment

The NOI responses note the following market benefits of open architecture deployment:

"The flexibility, growth, and performance benefits of a software defined stack is best leveraged with an open, modular hardware baseline that allows re-architecting." Spectranetix / Pacific Defense / US Army

- Better opportunities for innovation
- Supports experimentation on specific components
- Fosters the creation of a diverse and competitive RAN supplier ecosystem
- Potentially shortens product development cycles, improving time to market
- Enhances the ability to take advantage of evolving 3GPP specifications

And the following benefits for network operators:

- Potentially improves performance, via best of breed vendor selection
- Improves network flexibility
- Prevents vendor lock-in
- Reduces costs, especially for new capabilities
- Improves visibility of security data and security events
- Improves ability to monitor and control security response
- Faster security patch installation
- Enables agile approach to upgrades (i.e., reduces the need to physically replace equipment)

Potential Impediments to 5G Open Architecture Deployment

The NOI responses note that single-vendor, non-open, end-to-end solutions will have strong advantages in early 5G deployment:

"While incumbent suppliers will publicly support open interfaces, in practice, such suppliers have no incentive to ensure their adoption and success in the market." Dell

- Better support
- Better perceived maturity
- Coherent development of end-to-end solution
- Finances and market share
- Access to 5G testbeds, network emulators, etc.

The respondents also noted what are perceived as disadvantages of open interface solutions:

- Piecemeal growth
- Potential for slower development
- Latency and scalability
- Complexity of integration and deployment
- More complex maintenance, to include fault finding and remediation, during operation
- Lack of end-to-end coordination for optimization and upgrades

Benefits of Removing Barriers to 5G Open Architecture Deployment through a 5G Challenge

"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." AT&T

The NOI responses identified the following benefits of a 5G Challenge for exploring potential solutions to 5G open architecture challenges:

- Demonstrate the viability of open interfaces to the public sector and other governments
- Establish market expectations
- Promote an innovative ecosystem of trusted US and allied providers
- Accelerate commercial vendor ecosystem growth
- Address security concerns around open architectures
- Ensure the 5G stack meets DoD needs
- Improve network flexibility through modularity and interoperability
- Prevent vendor lock-in when changing, expanding, or upgrading networks

Enable Vendor Diversity in Commerce

Respondents encourage the challenge team to support vendor diversity, with a focus on helping new companies of all sizes enter the 5G market. This could enable a future with multiple vendors for each 5G network component. Various mechanisms are proposed whereby the challenge team could offer financial support, software tools, laboratory access, or subject matter expertise to US companies.

Support New Participation

Responses frequently expressed the need to help new companies enter the 5G market. Respondents would like the challenge team to encourage smaller companies to participate and demonstrate their unique capabilities. Respondents raise a concern that innovation opportunities tend to be biased toward large companies.

"The 5G Challenge needs to address integration of hardware and software stack components from both large players as well as small innovators who may have deep expertise in a specific component of the 5G stack." Cirrus360

The challenge team could enable innovation by providing support for the decomposition of standard functional interfaces into smaller components, to meet DoD needs that exceed commercial needs. These components are not typically developed to open interface standards.

Advancing the development and testing of infrastructure and software tools are critical to fostering a vendor diverse 5G open architecture ecosystem. The challenge team is encouraged to develop a 5G testbed, an open-source test suite, and "gateware" tools to foster collaboration.

5G Testbed

A **testbed** is a physical laboratory that contains one or more real 5G networks. A component's performance is evaluated with actual 5G network equipment.

New participants need easy access to a 5G testbed, a lab where they can test interoperability without waiting for a "plugfest" or partnering with a large company. A **plugfest** is an event where multiple vendors test interoperability and standards conformance by plugging their equipment together. The NOI responses express the need for development support for US industry, not certification testing. Additional recommendations include minimal contractual requirements,

allowing unbiased access to the testbed, a vendor neutral environment, and remote access capabilities.

Many NOI responses mention this need, as well as the existence of the National Science Foundation (NSF) testbeds. The implication is that existing testbeds did not fully serve US industry needs at the time of the NOI.

5G Test Suite

A **test suite** is a software-based solution that evaluates whether the function interface conforms to a standard. Test suites evaluate the component's interface in isolation.

NOI responses note the need for a 5G test suite. This would enable systematic functional testing across all 5G interfaces and organizations. The test suite would support validation testing and deployment, where open interface solutions struggle. A test suite will be needed for interoperability validation in this challenge. The test suite could also be used to evaluate performance and scalability.

"...focus on extensive functional testing of all relevant (external, interoperable) interfaces. Such testing should ideally be performed against a to-be-created open source test suite..." sysmocom

Some NOI responses express specific support for more development of open-source 5G test suites. An open-source test suite would allow all companies to perform their own self-certification—generic test cases in a cloud-based lab—before undergoing more time consuming and expensive interoperability testing. An open-source solution would help all users agree upon automated testing of high-risk function points.

5G Network Emulation

Systems exist that emulate part or all of the 5G network, although they are missing some components of a full end-to-end network deployment.

Softwarization, Gateware, and Performance Drops

"Motivating the large Chipset and Device manufacturers to break up their stacks for others to compete for each layer may not be initially welcomed. In addition, technology available today for real time processing between layers may not support this division." Keysight

The NOI responses encourage the challenge team to support **softwarization**—5G software solutions that can be run on white-box hardware. The communications industry has already shifted from a hardware centric model toward software defined networks and more open interfaces.

The respondents identify the problem of how to support softwarization while avoiding a reduction in performance when interoperating in a multi-vendor environment. Some NOI respondents noted that the 5G requirements for high bandwidth and ultra-low latency features may be easier to implement when the software and hardware are designed jointly. For example, software may have the ability to run faster if it is designed for a specific hardware platform. Other respondents noted that network operators are already moving from hardware centric solutions to softwarization, which takes better advantage of advances in silicon, software, and cloud to improve performance.

"[The] lack of high-quality free and open source software tools for gateware design hampers efficient collaboration in this domain." Open Source Hardware Association (OSHA)

Additional hardware-centric feedback focused on gateware. One respondent noted that new participants to the 5G market would have an easier time taking advantage of field-programmable gate array (FPGA) chips if provided with improved gateware tools. **Gateware** is hardware description language (HDL) for programming FPGAs and application-specific integrated circuit (ASIC) chips.

Security

Overall, respondents note that 5G technology has the potential for security improvements and that security must be integral to the software development. This means establishing a software factory framework and using DevSecOps processes. Recommended best practice for secure software development, like all 5G software development, is a continuous integration / continuous delivery (CI/CD) model. This is mostly the vendor's responsibility, but respondents encouraged the challenge team to adopt and promote a software factory framework model based on existing DoD efforts.

Respondents stressed the importance of good practices on network security—a 5G network operational security framework using zero trust architecture, visualization, and automation for corrective action control.

Offline compliance and analysis tools were also identified as needs. Respondents want an inventory of the available tools, best practices, and known security risks. This framework would identify tools for a software bill of materials (SBOM), X-Apps for O-RAN, security audits, and vulnerability analyses.

"When malicious traffic is detected, a honeypot slice will be created automatically, and the malicious traffic will be transported on the honeypot slice." AT&T

Additional security-centric feedback focused on improving 5G security by seeking ways to support the utilization and development of 5G security honeypots within the bounds of the challenge process. Honeypots provide a "hacker's paradise" designed to entice hackers and isolate their activity. It was noted that 5G security could also be enhanced by the creation of a supply chain of trusted vendors for all 5G network systems.

Prize Challenges

Prize Challenge Goals

The NOI responses contain no obvious trends around prize challenge goals. High level concepts such as network slicing, security, resilience, efficiency, latency, scalability, interoperability, reliability, and virtualization were referenced as outcome-based focus areas. In the NOI responses, no respondent called for a single, stand-alone prize.

Multiple Prize Challenges

The pattern of prize challenge goal responses indicates that the best way to encourage new participation and faster maturation of open 5G technology will be a series of targeted prize challenges on different topics. Prize challenges should allow innovation from smaller companies, as well as larger companies. The challenge team is encouraged to consider phased activity with opportunities for diverse participation. Achieving a viable and impactful 5G Challenge program will require a software development life cycle approach. Evaluation of the goals, awards and outcomes of the program should be ongoing, and influenced by evolution of the 5G ecosystem, which will change rapidly over the next 2 to 5 years.

"By offering multiple challenges, the Government encourages greater participation with a broader collection of companies and organizations while driving innovation and decoupling the success of any one challenge area with another."
Booz Allen Hamilton, Inc.

Plugfest

Several NOI responses mention the value of previously held plugfests or the value of plugfests in general. Suggested values of plugfests that can assess and demonstrate the interoperability of 5G componentry are:

- Build esprit de corps
- Understand state of the art
- Capture issues faced by participants and design solutions
- Identify roadblocks and gaps to achieving wider diversity and integration
- Assess the maturity, reliability, and scalability of components
- Encourage vendors to contribute to open interfaces and open architecture within their area of expertise
- Motivate improvement and innovation
- Enable collaboration among vendors
- Reduce market access barriers

Prize Challenge Structure

The NOI responses indicate that the goals and structure of a prize challenge are interdependent. These terms were not clearly defined in the NOI, leading to ambiguity. The following trends were observed.

Prizes and Incentives

Several common themes emerged with respect to prizes and incentives. Respondents suggested that:

- Prize challenges should be structured to encourage collaboration and market diversity
- The more popular "winner" structure is inadvisable
- Prizes could be proportional to the level of interoperability
- Winners could be provided with public recognition through awards and certifications at the conclusion of the challenge.

The challenge team is encouraged to leverage other federal 5G programs or to provide financial support and federal economic incentives for participants.

"The ultimate goal of this contest should not be to declare a winner. Rather, it should be to establish a vibrant and self-sustaining ecosystem with accelerated innovation and enhanced security." Google

"The proposed challenge is based on 'Coopetition'—which signifies competition in the same horizontal (e.g. among various compliant MIMO radio vendors) but collaboration across vertically connected network stack elements..." OpenAirX-Labs

The challenge team is also encouraged to demonstrate a path to commercial use for the technologies involved. This could include coordinating with federal efforts to deploy 5G infrastructure in and on federal facilities, as well as commercial buildings.

See also the discussion of 5G testbeds.

Teams

The NOI responses support mechanisms for multiple team collaboration, meaning prize challenge rules and testbeds that will allow co-development between people in different organizations. It is recommended that partnerships demand minimal or no contractual requirements, and that companies and respondents be able to support multiple teams with varying elements of a 5G architecture.

DoD Use Cases

To help participants understand unique DoD needs, it is recommended that, where possible, prize challenges describe specific DoD use cases.

RAN Space

Responses point out that the RAN space is typically underrepresented in the open 5G stack. The cost of radio units coupled with inexperience with the hardware is cited as making this the most challenging area for newcomers. Thus, it is recommended that the challenge seek to overcome this obstacle by providing emulated environments and 5G radio testbeds. This would remove the need for smaller RAN solutions to develop their radio frequency (RF) hardware in-house.

User Equipment

Little consideration is given to user equipment (UE) in the NOI responses.

A few NOI responses recommend focusing specifically on the new 5G capabilities that will enable new products and services of interest to DoD (e.g., high bitrate, low latency). By implication, such challenges must be implemented later, when the UEs can at least be emulated.

"...[incorporate] as many 5G-related, practical, real-world applications as is feasible...a low latency application, a high reliability application, a high bandwidth application, and a large scale (number of devices) application." NEC

Existing Technologies

Many of the NOI responses provide extensive background information that will help newcomers learn about 5G. This information may be limited to a specific organization's 5G endeavors or may provide a broad overview of certain aspects of the 5G market. Refer here for NOI responses that provide such background information.

Container platforms are available that underpin cloud native infrastructure, automation, and orchestration. It was pointed out that these individual components would benefit from a focus on integration and testing as part of a 5G challenge.

Where possible, the challenge team is encouraged to leverage ongoing endeavors of other organizations. Examples include the NIST Cybersecurity Framework and the Telecom Infra Project (TIP) Field Trials. DoD and NTIA are also advised to leverage open-source projects (e.g., Kubernetes, OpenStack, Antrea, and Open V-switch). These may provide suitable benchmarks for evaluation criteria.

Infrastructure

The NOI responses propose selecting a reference solution and making it available to participants, as this would allow smaller companies to develop niche or smaller scale solutions and test with the rest of the stack. An emulated 5G network may be suitable for challenges that do not involve radio units.

The NOI responses emphasize the need for 5G testbeds and a 5G test suite. Recommended testbed hardware includes white-box servers, white-box processors, hardware accelerators, distributed cloud platforms, and radio units. Details of quantity and performance are not provided.

Timeframe

Recommendations for challenge timeline diverge significantly, with some being as short as 12 months and others suggesting four years. The most common answers are on the order of two to four years. The first phase (requirements development, setup, or introduction) is commonly given 6 to 12 months. Phase 2 (basic functionality demonstrations) would extend 6 to 12 months beyond phase 1. Phase 3 (more advanced, challenge specific, interoperability, or shortlisted demonstrations) would extend 6-12 months beyond phase 2.

NOI Responses Summary

Table 1 provides a high level summary of the NOI responses. The columns in this table are as follows:

- **Respondent**: Name of the company, university, organization, or person who submitted the response. The NOI response file name begins with this text.
- **Role:** Brief overview of the respondent, taken from internet searches.
- **Pages:** Length of the NOI response, in pages
- **Style:**

Q&A	directly answers the NOI questions
1off	one-off, creative brainstorming
BG	background information
ENG	engagement recommendations
INV	innovation ideas other than prize challenges
HL	high level insights
N	negative / unsupportive

TABLE 1. NOI RESPONSE SUMMARY

Respondent	*Role*	*Pages*	*Style*
5G Americas	*Industry trade organization*	*60*	*ENG, BG*
5G Open Innovation Lab	*US based, private public partnership*	*7*	*BG, Q&A, ENG*
Aarna Networks Inc.	*US based, open-source software*	*6*	*BG, Q&A, INV*
ACT – The APP Association	*Consortium of small business app & IoT developers*	*8*	*BG, 1off*
Airspan	*US based, RAN tech company*	*2*	*1off, ENG*
Altiostar	*US based, 4G and 5G open virtualized RAN (Open vRAN) software*	*10*	*Q&A*
Anne Wilder	*Individual*	*5*	*N*
AT&T Services	*US based, telecom company*	*13*	*Q&A, BG*
Avanti	*US owned / UK based satellite owner & operator*	*1*	*BG*
Booz Allen Hamilton Inc.	*Consulting company*	*9*	*1off*
Cable Labs	*Not for profit innovation & R&D lab for cable industry*	*5*	*HL*
CACI, Inc.	*US based company, provides services to DoD*	*1*	*Q&A*
Cirrus360 Corp	*US based company, edge computing*	*6*	*BG, Q&A*
Dell Technologies	*US based company, computers etc.*	*5*	*BG, Q&A, INV*
Ericsson	*Swedish / US based, networking & telecom*	*19*	*INV, BG, Q&A*
Fujitsu	*Japanese / US based, computing products & services*	*5*	*BG*
GitHub	*Internet hosting for software*	*5*	*ENG, Q&A*

Respondent	Role	Pages	Style
Google	US based tech company, internet services & products	4	BG, ENG, HL, 10ff
IBM	US based tech company	3	HL, Q&A
Illuminate Mission Solutions	US based company, network monitoring	2	HL, BG
Indiana 5G Zone	US based, NineTwelve Institute (NTI) collaborative	17	Q&A
Infiltron Software Suite	US based company? Security	4	BG
Information Technology Industry Council	US based advocacy	3	10ff, ENG
Intel	US based tech company	2	BG, ENG
InterDigital Communications Inc.	US based, mobile tech R&D	3	Q&A
Juniper Networks	US based, 5G Core Focused Manufacturer.	6	BG
Keysight	US based, test equipment for 5G	2	10ff, HL, ENG
Krista Hess-Mills	Individual	1	N
Linux Foundation	US based, non-profit, supports open-source tech	6	BG, HL, ENG, Q&A
Lockheed Martin	US based company: aerospace, arms, defense, security, advanced technologies	14	Q&A
Mavenir System Inc.	US based company, mobile network solutions, LTE & 5G	8	HL, BG
NASA	Federal agency	4	BG, HL, ENG, Q&A
National Spectrum Consortium	US based consortium, 5G collaboration	8	BG, HL
NEC	Japanese company, IT & networking	5	BG, 10ff
Northeastern University	US university	6	Q&A
Open RAN Policy Coalition	Industry coalition	5	HL
Open Source Hardware Association	Advocacy organization	3	BG, ENG, 10ff
OpenAir-X Labs	US based consortium	17	Q&A
Prizm XR	US based, small business	5	Q&A
Rakuten	Japanese based e-commerce (and mobile) company	4	BG, Q&A
Red Hat	US based open-source software company	5	10ff, INV, BG
River Loop Security	US based cybersecurity company	3	10ff, BG
Robin Welker	Individual	1	N
SLA Labs	Unknown / dead website	18	Q&A, BG
Spectranetix / Pacific Defense / US Army	CRADA collaboration group	5	BG, 10ff
sysmocom	German company, open-source mobile communications	6	BG, Q&A

Respondent	Role	Pages	Style
T-Mobile	US based wireless network provider	14	N
Telecom Infra Project (TIP)	Non-profit convening organization	20	BG, 1off, ENG
Tony Rutkowski	Individual	1	N
University of Texas at Dallas, Open Network Advanced Research Lab	US based, public research university	4	1off, BG, INV, ENG
VMware	US based, cloud and virtualization software company	8	Q&A, BG, ENG

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
July 29, 2021	NTIA Special Publication	1/11/2021	2/16/2021

4. TITLE AND SUBTITLE
5G Prize Challenge Notice of Inquiry Analysis

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
5a. PROJECT NUMBER	**5b. TASK NUMBER**	**5c. WORK UNIT NUMBER**
6922000	300	NTIA/ITS.P

6. AUTHOR(S)
Margaret Pinson, Julie Kub and Jeremy Glenn

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
National Telecommunications and Information Administration Institute for Telecommunication Sciences 325 Broadway Boulder, CO 80305	SP-21-554

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER(S)
U.S. Department of Defense Office of the Under Secretary of Defense Directorate for Modernization Research and Engineering (USD(R&E)) The Pentagon, Washington, DC 20301	OUSD R&E DDRE(M)	

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release. Distribution Unlimited.

13. SUPPLEMENTARY NOTES
Related Notice of Inquiry FR Doc. 2021–00202, 86 FR 1949

14. ABSTRACT
This document provides an analysis of responses to the 5G Challenge Notice of Inquiry (NOI) issued by the National Telecommunications and Information Administration (NTIA) on behalf of the Department of Defense (DoD). This analysis was created by NTIA's Institute for Telecommunication Sciences (ITS) to inform future collaborations between the DoD and NTIA. This analysis will feed into the creation of a 5G Challenge and Incentive Program that accelerates the maturity of 5G open interfaces and between vendor module interoperability. This will allow new participants to enter the 5G market.

15. SUBJECT TERMS
5G, emulation, gateware, notice of inquiry (NOI), open architecture, open interface, open RAN, open source, plugfest, prize challenge, softwarization, testbed

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	c. THIS PAGE		
Unclassified	Unclassified	Unclassified	Same as Report	16

19a. NAME OF RESPONSIBLE PERSON	19b. TELEPHONE NUMBER *(Include area code)*
ITS Publications Officer	303-497-3572

PREVIOUS EDITION IS OBSOLETE.

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18