Before the Department of Commerce
National Telecommunications and Information Administration
Washington, D.C.

In the Matter of

Public Wireless Supply Chain Innovation	)	NTIA-2022-26938
Fund Implementation	)	Docket No. NTIA-2022-0003
	)	

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

January 27, 2023

Table of Contents

I. INTRODUCTION AND EXECUTIVE SUMMARY

CTIA[1] appreciates the opportunity to provide input on NTIA's Request for Comment ("RFC") about the implementation of the Public Wireless Supply Chain Innovation Fund ("Innovation Fund").[2] The Innovation Fund was created by the 2021 National Defense Authorization Act ("2021 NDAA"), and the fund aims to aid in promoting and deploying "open and interoperable interface radio access networks."[3] The National Telecommunication and Information Administration ("NTIA") administers the Innovation Fund. On August 9, 2022, the CHIPS and Science Act of 2022 ("CHIPS Act") became law, appropriating $1.5 billion for the Innovation Fund.[4] In this RFC, NTIA seeks comment on implementation of the fund.

CTIA supports industry leadership, provider choice, and competition as the best way to promote a future of secure and innovative networks. This future, due in no small part to the leadership of CTIA's member companies, will include Radio Access Networks with standardized open and interoperable interfaces ("Open RAN"). The global market and technical standards processes are driving advances in Open RAN, and this progress is accelerating in the broader context of 5G network deployments.

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, and suppliers, as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Public Wireless Supply Chain Innovation Fund Implementation*, Notice and Request for Comment, 87 Fed. Reg. 76182-85 (Dec. 13, 2022), https://www.federalregister.gov/documents/2022/12/13/2022-26938/public-wireless-supply-chain-innovation-fund-implementation ("RFC").

[3] 47 U.S.C. 906(a)(1)(C)(i).

[4] CHIPS Act of 2022, Pub. L. No. 117-167, § 102(c), 136 Stat. 1366, 1375-77 (2022), https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf.

Federal support can advance Open RAN development. NTIA's implementation of the Innovation Fund should recognize the complex dynamics that will contribute to Open RAN development, including market competition and advances in technical standards and interoperability. Development of Open RAN is complex because multivendor deployments present integration and other practical challenges. Deployment of Open RAN will occur as market participants, in particular network operators, see that it can scale and will not negatively impact performance or feature parity. To ensure that advances continue, Congress directed NTIA to promote a diverse, competitive global market of trusted suppliers within the United States and its partners and allies worldwide. As described herein, CTIA supports broad eligibility for funding to companies in trusted and allied countries.

In these comments, CTIA recommends that NTIA avoid interfering with provider choice in how to design their networks, and the agency should not use the Innovation Fund to subsidize deployment or equipment purchases by any network operator. Network security and reliability are imperatives, and NTIA should encourage providers to deploy Open RAN as appropriate for their networks and deployment timelines. Encouraging providers to determine the time and manner of any Open RAN deployment will help ensure network security and stability. NTIA should encourage providers to take a flexible, risk-based approach to Open RAN deployments and advanced threat detection and mitigation, to ensure use of 3rd Generation Partnership Project ("3GPP") 5G standards, O-RAN Alliance specifications, and other best practices.

CTIA also recommends that NTIA use the Innovation Fund to focus on technology development and helping solve practical challenges. This can include research and work on interoperability, as well as the promotion of equipment that meets specifications like those from the O-RAN Alliance, and projects that support hardware design and energy efficiency. Such projects could focus on the development of hardware designs that have better energy efficiency including small form factors. These projects are particularly important for RU deployments (including macro, micro, and small cell deployments) and could support Open RAN component manufacturers. NTIA also can address challenges in systems integration, to help make Open RAN a viable choice for operators and support innovation. As part of this work, NTIA can explore funding of positioning, navigation, and timing ("PNT") Open RAN projects, test bed work, and pilot programs, among other efforts.

II. THE WIRELESS INDUSTRY IS ADVANCING OPEN RAN DOMESTICALLY AND GLOBALLY.

CTIA members are driving global advances in 5G technical standards through 3GPP, the world's preeminent standards body for cellular technologies, and on open and interoperable RAN through the O-RAN Alliance. In fact, several of CTIA's members are leading members of the O-RAN Alliance.

Openness has been a hallmark of the wireless industry, and it will shape the future of 6G and beyond. Technological advances generally trend toward standardized open and interoperable interfaces between different network components. This trend towards openness has driven initiatives such as the Open Network Automation Platform ("ONAP"), as well as 3GPP, which developed the standards for 5G and the continuing evolution of advanced telecommunications.[5] In addition, the O-Ran Alliance is developing specifications for open interfaces between various subcomponents in the RAN.[6] As NTIA develops Notices of Funding Opportunity ("NOFOs") for the Innovation Fund, it should promote private deployment of rigorously vetted open standards and deployment of equipment and networks compliant with

[5] *See* 3GPP, https://www.3gpp.org/ (last accessed Jan. 24, 2023).

[6] *See* O-RAN Alliance, https://www.o-ran.org/ (last accessed Jan. 24, 2023).

these standards and specifications. Federal telecommunications policy has long championed global, open, and transparent standards and specifications that promote interoperability.

In NTIA's development of NOFOs, it should tailor funding to help define concrete steps to expedite the deployment and integration of Open RAN systems. Specifically, NTIA should focus on promoting research and development ("R&D") to validate Open RAN functionality, interoperability, scalability, and ease of system integration. NTIA should not pursue subsidy programs for the purchase and use of Open RAN in commercial networks.

III. NTIA SHOULD PROMOTE FLEXIBILITY AS IT DEVELOPS NOFOS.

A. NOFOs Should Generally Provide Grantees with Flexibility.

CTIA welcomes the Innovation Fund and complementary federal efforts to support Open RAN. To best promote Open RAN, NTIA should provide grantees with flexibility to build safe and trusted Open RAN. As NTIA develops NOFOs, it should avoid any mandates or technical preferences. The federal government generally, and NTIA specifically, should not pick winners and losers or take action that will distort market forces in network deployment.

Open RAN work in the wireless industry is underway and will be deployed as network operators expand and update their networks, when investment cycles align with the ability of Open RAN to scale and to support network performance and feature parity. National providers have contracts in place for their 5G buildouts, and builds are ongoing. Government intervention may disrupt deployment of 5G. Mandates to use particular deployment approaches could disrupt 5G transitions and may not meet the performance criteria of existing networks. Instead, Open RAN deployments should proceed according to providers' network demands and the type of Open RAN offerings they are considering. NTIA should ensure that providers have flexibility in using any NOFO funds for Open RAN implementation and avoid any prescriptive requirements.

B. Supply Chain and Eligibility Requirements Should Not Be Prescriptive or Narrow, so NTIA Can Ensure that Innovation Fund Programs Support Work with Trusted and Allied Companies Across the Globe.

NTIA seeks comment on proposed sourcing and eligibility requirements that may limit the types of projects that would be available for funding. Specifically, the RFC asks a series of questions about the global supply chain for Open RAN equipment, as well as whether NTIA should require that grantee projects take place in the United States or whether NTIA should ensure that "American-made" network components are utilized.[7] NTIA also asks if it should "collaborate with like-minded governments to achieve Innovation Fund goals."[8]

The Innovation Fund presents an opportunity to help build a global and trusted open standards-based ecosystem, and NTIA should promote a diverse global market of trusted suppliers based in the United States as well as with allies and partners. The U.S. market presently is not large enough to support the diversity of trusted suppliers that CTIA's provider members or its vendor members need. Although CTIA strongly supports efforts to enhance domestic development and manufacturing capabilities, NTIA must take a broader perspective if the goals of the Innovation Fund are to be achieved. Accordingly, NTIA should avoid tunnel vision when pursuing greater O-RAN supply chain competitiveness, and should not narrowly focus on U.S. manufacturing or limit opportunities to the U.S. market. Specifically, any requirement for equipment to be "American-made" would be problematic, since it could refer to where a company is headquartered, manufactures, or develops software—which are different concepts. To avoid confusion and friction, NTIA should not include any requirements mandating the use of "American-made" components.

[7] RFC 5, 25(a)-(c).

[8] RFC 26.

To promote U.S. interests in Open RAN and supply chain resilience, a global market perspective is necessary. As Open RAN policies are developed, NTIA should view the success of Open RAN as a global effort that will require friendly markets among and between the United States and its global partners. NTIA should expressly seek to advance a diverse, competitive market of trusted suppliers based in the United States, allied nations, and other partner market democracies and like-minded nations. Allies include NATO countries, non-NATO European partners, Five Eyes allies, Japan, South Korea, Israel, and India.

While the United States should engage its allies in promoting Open RAN policies, the Multilateral Fund, and not the Innovation Fund, appears to be the best vehicle for tackling global Open RAN supply chain issues directly with allied and overseas partners. The Innovation Fund promotes the development of Open RAN technology generally; the focus of the Innovation Fund is to create conditions in which Open RAN systems flourish and promote competition in wireless infrastructure. Federal funding can improve competitiveness in 5G and successor wireless technology supply chains that use Open RAN equipment *without* creating strict supply chain sourcing requirements.[9] Notably, the Multilateral Fund explicitly addresses telecom supply chain and security issues through commitments with trusted foreign partners.[10] The Multilateral Fund's implementation requires the Secretary of State to reach agreements with foreign partners to create a common funding mechanism. If NTIA were to delve into complex supply chain

[9] *See* 47 U.S.C. 906(a)(1)(C)(i) (explaining that one of the goals of the Innovation Fund is "Promoting and deploying technology, including software, hardware, and microprocessing technology, that will enhance competitiveness in the fifth-generation (commonly known as '5G') and successor wireless technology supply chains that use open and interoperable interface radio access networks.").

[10] 47 U.S.C. 906(a)(2)(B) (noting that "In creating and sustaining a common funding mechanism, the Secretary of State should leverage United States funding in order to secure commitments and contributions from trusted foreign partners such as the United Kingdom, Canada, Australia, New Zealand, and Japan, and should prioritize the following objectives: (i) Advancing research and development of secure and trusted communications technologies. (ii) Strengthening supply chains. (iii) Promoting the use of trusted vendors.").

sourcing requirements in NOFOs, it may limit or get ahead of State Department involvement in telecommunications supply chain-related funding initiatives.

Accordingly, NTIA should not create supply chain-related sourcing requirements as it develops NOFOs. The Multilateral Fund, and not the Innovation Fund, is better suited to handle supply chain issues related to telecommunications equipment, including Open RAN components. If NTIA chooses to explore any "American-made" or other component sourcing requirements, it should provide grantees with flexibility. Grantees should have the flexibility to source equipment and components from trusted vendors from allied countries, and not be confined to domestically produced components.

Likewise, NTIA should avoid fragmentation with the numerous other federal efforts on the supply chain, which could create supply chain disruptions. Many federal workstreams address information and communications technology ("ICT") supply chain issues. NTIA has published the minimum elements for a Software Bill of Materials.[11] The Federal Communications Commission ("FCC" or "Commission") has issued several orders to address ICT supply chain integrity by prohibiting the use of federal universal service funds for communications equipment and services provided by entities that pose a threat to national security.[12] The FCC also recently restricted the use of the Commission's equipment authorization process by certain high-risk entities.[13] The Department of Commerce

[11] Department of Commerce, National Telecommunications and Information Administration, *The Minimum Elements For a Software Bill of Materials (SBOM)* (July 12, 2021), https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

[12] *See, e.g.*, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Proposed Rule, 86 Fed. Reg. 15,165 (Mar. 22, 2021), https://www.federalregister.gov/documents/2021/03/22/2021-04692/protecting-against-national-security-threats-to-the-communications-supply-chain-through-fcc-programs (implementing a reimbursement program to expedite removal of harmful equipment and services).

[13] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through*

("Department") issued an interim final rule on review of ICTS transactions and is working on an advance licensing process for certain transactions.[14] The Department also issued an RFC on supply chains for the ICT industrial base to inform a report to the President.[15] And the Department of Homeland Security ("DHS") ICT Supply Chain Risk Management ("SCRM") Task Force has been addressing cyber threats to ICT supply chains.[16] If NTIA addresses supply chain issues, it should aim to harmonize any supply chain requirements with these ongoing supply chain efforts to avoid creating uncertainty or supply chain shocks.

Related to the issue of eligibility, NTIA should include CTIA members on any list of trusted vendors. To accelerate the growth of Open RAN, any NTIA programs should lean on a trusted allied market. In order to move quickly at scale, allied vendors should be included in NTIA Open RAN programs. The FCC's Communications Security, Reliability, and Interoperability Council ("CSRIC") has stated, "Open RAN includes O-RAN, Virtual RAN (vRAN), Cloud RAN, and other technologies."[17] Numerous vendors—and CTIA members—are

the Competitive Bidding Program, ET Docket No. 21-232, EA Docket No. 21-233, Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84 (Nov. 25, 2022), https://docs.fcc.gov/public/attachments/FCC-22-84A1.pdf.

[14] *Securing the Information and Communications Technology and Services Supply Chain*, Interim Final Rule and Request for Comment, 86 Fed. Reg. 4,909 (Jan. 19, 2021), https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain; *Securing the Information and Communications Technology and Services Supply Chain: Licensing Procedures*, Advanced Notice of Proposed Rulemaking, 86 Fed. Reg. 16,312 (Mar. 29, 2021), https://www.federalregister.gov/documents/2021/03/29/2021-06529/securing-the-information-and-communications-technology-and-services-supply-chain-licensing.

[15]*Notice of Request for Public Comments on Risks in the Information Communications Technology Supply Chain*, Notice of Request for Public Comments, 86 Fed. Reg. 52,127 (Sept. 20, 2021), https://www.federalregister.gov/documents/2021/09/20/2021-20229/notice-of-request-for-public-comments-on-risks-in-the-information-communications-technology-supply.

[16] CISA, *ICT Supply Chain Risk Management Task Force*, https://www.cisa.gov/ict-scrm-task-force (last accessed Jan. 24, 2023).

[17] CSRIC VIII, Report Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment, at 4 (Dec. 2022), available at https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-1 (last accessed at Jan. 23, 2023) ("CSRIC Open RAN Report").

developing and deploying offerings that advance virtualized RAN and cloud-based capabilities that will facilitate the transition to Open RAN.[18]

NTIA should look to fund programs that promote competitiveness and include trusted vendors. Further, The NOFOs should recognize that Open RAN can take a variety of forms, and operators utilizing the Innovation Fund should be able to choose any Open RAN technology. Additionally, applicants to any NOFOs from this proceeding should be able to partner with other organizations to fulfill any obligations. For example, applicant providers should be able to team with trusted vendors when seeking funding for certain projects.

C. NTIA Should Not Create Burdensome Security Reporting Requirements.

The RFC asks about security reporting and the role that security industry standards, best practices, and frameworks should play in any NOFOs.[19] NTIA should not include any overly prescriptive security-related certifications in NOFOs. Numerous federal workstreams are addressing security reporting, and NTIA should avoid duplicating federal efforts, or it should attempt to harmonize with existing reporting requirements. There are developing federal workflows addressing ongoing security efforts. For example, DHS's Cybersecurity and Infrastructure Security Agency ("CISA") is developing reporting requirements for critical infrastructure entities, such as the communications sector under CIRCIA.[20] The FCC recently

[18] *See, e.g.*, Ericsson, *Cloud RAN*, https://www.ericsson.com/en/ran/cloud (last accessed Jan. 24, 2023); Intel, *Virtualizing the Radio Access Network*, https://www.intel.com/content/www/us/en/communications/virtualizing-radio-access-network.html (last accessed Jan. 24, 2023); Nokia, *AirScale Cloud Ran*, https://www.nokia.com/networks/solutions/airscale-cloud-ran/ (last accessed Jan. 24, 2023); Press Release, Qualcomm, Qualcomm Builds Momentum for Full-Scale Open RAN Commercialization with the Sampling of its 5G RAN Platforms (Sept. 28, 2022), https://www.qualcomm.com/news/releases/2022/09/qualcomm-builds-momentum-for-full-scale-open-ran; Press Release, Samsung, Samsung Achieves Industry First: Expands Virtualized RAN Capability to Support C-Band Massive MIMO Radio (June 8, 2021), https://news.samsung.com/us/samsung-achieves-industry-first-expands-virtualized-ran-capability-support-c-band-massive-mimo-radio/.

[19] RFC 17(a)-(b), 19.

[20] Consolidated Appropriations Act, 2022, Pub. L. 117-103, Div. Y, 136 Stat. 49, 1038-1059 (2022), https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf ("CIRCIA"); *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Request for Information, 87 Fed. Reg. 55,833

released a Notice of Proposed Rulemaking that would modify customer proprietary network information ("CPNI") breach reporting rules.[21] Further, the FCC recently proposed to require Emergency Alert System ("EAS") participants to report to the FCC any incident of unauthorized access of its EAS equipment "within 72 hours of when it knew or should have known that an incident has occurred."[22] Communications providers are also required to report certain outages within various timeframes according to the type of provider.[23]

NTIA should avoid contributing to cybersecurity reporting fragmentation by creating additional burdensome reporting requirements. If NTIA, however, decides to include reporting requirements for Innovation Fund disbursements, it should tailor expectations to the project at issue and harmonize any requirements in coordination with other federal agencies. Any security-related certifications for Innovation Fund use should not be more stringent than any such NIST best practices. NOFOs, if they contain security requirements, should tie any certifications to NIST best practices, such as the Cybersecurity Framework, which enshrines flexibility.

D. NTIA Should Not Promote Inflexible Zero Trust Practices.

NTIA is interested in zero trust, and it seeks input on how zero trust concepts may inform its work on the Innovation Fund. Specifically, the RFC asks, "How is the 'zero-trust model' currently applied to 5G network deployment, for both traditional and open and interoperable, standards-based RAN? What work remains in this space?"[24]

(Sept. 12, 2022), https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022.

[21] *Data Breach Reporting Requirements*, WC Docket No. 22-21, Notice of Proposed Rulemaking, FCC 22-102 (Jan. 6, 2023), https://docs.fcc.gov/public/attachments/FCC-22-102A1.pdf.

[22] *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert Systems et al.*, PS Docket Nos. 15-94, 15-91, 22-329, Notice of Proposed Rulemaking, FCC 22-82, at 8-9 (Oct. 27, 2022), https://docs.fcc.gov/public/attachments/FCC-22-82A1.pdf.

[23] 47 C.F.R. § 4.9.

[24] RFC 20.

The wireless industry has been using and innovating in zero trust. The wireless industry supported the development of mutual authentication techniques and has ensured that SIM cards are allocated unique identifiers, which allows devices to be authenticated as they travel throughout networks. The Alliance for Telecommunications Industry Solutions ("ATIS") has published—and continues to work on—standards for 5G that cover zero trust.[25] The telecommunications industry has been involved with the FCC's CSRIC[26] and 3GPP 5G security work involving zero trust.[27] CTIA recently released a zero trust white paper, *Defining Zero Trust: Industry Approaches and Policy Frameworks for Strong Wireless Network Security*.[28] The paper explains two key aspects of zero trust, namely, that flexibility is a fundamental part of zero trust, and zero trust is a process and not an end state.[29] NTIA should draw on CTIA's white paper if it considers any zero trust-related expectations for NOFOs.

While CTIA does not support technology-specific mandates in any NOFOs, if NTIA looks to incorporate zero trust principles in Innovation Fund activity, it should provide applicants

[25] *See, e.g.*, ATIS, ATIS-I-0000090, ATIS Standard: 5G Network Assured Supply Chain, at 82 (June 2022), https://access.atis.org/apps/group_public/download.php/66150/ATIS-I-0000090.pdf (explaining that the 5G Core network has been designed to incorporate a variety of zero trust capabilities across the network's architecture); ATIS, ATIS-I-0000082, Collaborative DevSecOps in a Service Provider Environment, at 30-33 (Mar. 2021), https://access.atis.org/apps/group_public/download.php/58287/ATIS-I-0000082.pdf. ATIS is also engaged in a new project that will analyze how 5G zero trust solutions can be integrated with other zero trust solutions through IT infrastructure. ATIS, *Enhanced Zero Trust and 5G*, https://www.atis.org/tops-council/enhanced-zero-trust-and-5g/ (last accessed Jan. 24, 2023).

[26] *See, e.g.*, CSRIC IV WG 4, Final Report: Cybersecurity Risk Management and Best Practices, at 261, 268, 280, 295 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf; CSRIC VII WG 4, Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG 9-1-1 Implementations, at 89 (Sept. 16, 2020) https://www.fcc.gov/file/19298/download.

[27] The FCC's CSRIC Working Group 2 has recommended that Open RAN implementations "should be based on the principles of Zero Trust Architecture (ZTA)." CSRIC Open RAN Report at 38. *See also* 3GPP, Technical Specification 33.894, Study on zero-trust security principles in mobile networks, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4086.

[28] CTIA, Defining Zero Trust: Industry Approaches and Policy Frameworks for Strong Wireless Network Security (2023), https://api.ctia.org/wp-content/uploads/2023/01/Defining-Zero-Trust-White-Paper-2023.pdf.

[29] *Id.* at 7.

with flexibility in implementation. NIST explains that "[zero trust] is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture."[30] CISA has likewise referred to zero trust as a "concept" and has provided recommendations for 5G cloud networks that would implement zero trust "principles."[31] As these agencies demonstrate and understand, zero trust is a security approach guided by principles and tenets, and not a set of requirements. Organizations have differing risk profiles and resources depending on their unique contexts. This diversity will limit the effectiveness of any across-the-board zero trust mandates. Accordingly, any zero trust-related expectations from NTIA should be risk-based and flexible. NTIA should not create rigid requirements for achieving zero trust or a zero trust architecture. Instead, NTIA should draw on NIST's flexible and risk-based guidance—such as NIST 800-207—on zero trust before pursuing any zero trust-related endeavors in its Innovation Fund NOFOs.[32]

IV. THE RFC ASKS IMPORTANT QUESTIONS ABOUT OPEN RAN DEVELOPMENT AND CHALLENGES IN DEPLOYMENT.

A. NTIA Should Champion O-RAN Alliance Specifications and 3GPP Standards.

NTIA seeks input about private sector initiatives that may be relevant to the Innovation Fund.[33] The wireless industry is involved in several such initiatives. CTIA members are driving global advances in 5G technical standards through 3GPP, the world's preeminent standards body

[30] NIST, Zero Trust Architecture, Special Publication 800-207, at 1 (Aug. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf ("NIST 800-207").

[31] *See, e.g.*, CISA, Security Guidance for 5G Cloud Infrastructures, Part IV: Ensure Integrity of Cloud Infrastructure, at 3 (2021), https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_IV_508_Compliant.pdf.

[32] *See generally* NIST 800-207.

[33] RFC 2.

for cellular technologies,[34] and on open and interoperable RAN through the O-RAN Alliance. Indeed, several of CTIA's members serve as leading members of the O-RAN Alliance. The specifications that are being developed by the O-RAN Alliance do not conflict with or compete against 3GPP standards. Instead, they build on and complement them. Global standards for 5G are developed within 3GPP and codified into sets of technical specifications called "Releases." 3GPP Release 15,[35] which was finalized in June 2019, provided the first specifications for 5G enhanced mobile broadband capabilities and outlined a new "disaggregated" RAN architecture that would split the traditional radio base station into two distinct components: the gNB-CU ("Central Unit") and gNB-DU ("Distributed Unit"). Building on 3GPP's Release 15, the O-RAN Alliance is working to define "open" specifications for the interfaces between disaggregated RAN components. O-RAN Alliance specifications are publicly available for download. The O-RAN Alliance has released specifications following Release 15, such as the "Minimum Viable Plan" that packages some of the already published specifications into a minimum viable set of Open RAN solutions for deploying commercial networks.[36] CTIA believes that these maturing specifications will assist in facilitating future Open RAN-compliant deployments.

In addition to general private sector initiatives, the RFC asks about the current state of Open RAN standards environments and whether those environments can improve "stability, interoperability, cost effectiveness, and market readiness."[37] Open RAN standards development

[34] *See* 3GPP, *Partners*, https://www.3gpp.org/about-3gpp/partners (last accessed Jan. 24, 2023).

[35] 3GPP, *Release 15*, https://www.3gpp.org/release-15 (last accessed Jan. 24, 2023).

[36] O-RAN Alliance, O-RAN Minimum Viable Plan and Acceleration towards Commercialization (June 29, 2021), https://assets-global.website-files.com/60b4ffd4ca081979751b5ed2/61199f8adc85474118cf6969_O-RAN%20Minimum%20Viable%20Plan%20and%20Acceleration%20towards%20Commercialization%20White%20Paper%2029%20June%202021.pdf.

[37] RFC 7.

is an international effort between companies across the globe in various standard-setting bodies. CTIA has historically championed industry participation in standards setting.

CTIA recommends that the U.S. government and the private sector work together to support Open RAN standards development. As NTIA explores the Open RAN standards environment, it should preserve the robust and open standards processes that U.S. policy has championed for decades. The United States should not attempt to serve as a top-down driver of technology advancement, in 5G generally or Open RAN specifically, or related standards development. As CTIA explained to NIST when it sought comment on foreign influence in global technical standards development, "[s]tandards should be developed through open processes that are transparent and driven by technical experts, advancing compatibility, innovation, and security. No country or company should control or unduly shape the direction of international standards processes."[38]

If NTIA focuses on work in 3GPP or the O-RAN Alliance, it should facilitate private sector participation. Promotion of greater private sector participation would help foster U.S. technological leadership and competitiveness. Collaboration with and through the private sector, rather than direct U.S. government engagement with international standards-setting bodies, helps private sector experts best advance Open RAN development and U.S. interests more generally.

B. NTIA Rightly Perceives Differing Challenges and Opportunities in Private and Public Sector Networks.

NTIA asks whether the private and public sectors face different challenges regarding the adoption and deployment of Open RAN.[39] Private sector entities must tackle unique challenges

[38] Comments of CTIA, *In the Matter of Study on People's Republic of China (PRC) Policies and Influence in the Development of International Standards for Emerging Technologies*, NIST Docket Number: 211026–0219 (Dec. 6, 2021), available at https://downloads.regulations.gov/NIST-2021-0006-0020/attachment_1.pdf

[39] RFC 1.

when deciding whether to deploy Open RAN in a network. These challenges may be particularly acute for larger operators, for which a move to Open RAN relies on scalability, performance, feature parity, and cost of operations. Simply put, a move to Open RAN must make financial sense and align with the cadence of network upgrades and buildout. System integration can be difficult due to the variety of vendors involved, necessarily, in an Open RAN system. Getting different components interoperable is one hurdle, but network management with multiple vendors presents its own challenges. For example, determining responsible parties in the event of an outage can be difficult, since there are multiple vendors involved in the network.

NTIA could explore vendor and operator experience with system integration, around which there is ongoing innovation. For example, NTT and Vodafone recently announced a Memorandum of Understanding that demonstrates a commitment to "cooperate towards harmonizing mobile operator system integration and test processes including testing criteria and experiences to create common test scripts, a series of software instructions needed to conduct a test. This uniform approach to testing will mean that vendors can avoid repetition when dealing with multiple operators, saving them time, capital outlays, and resources, also making sure the industry delivers, no matter the region, secure by design, high quality products as defined by the industry bodies - 3GPP and the ORAN Alliance."[40] NTIA could engage in outreach with vendors and operators to learn more about private sector experience with integration.

C. Interoperability Is a Key Challenge on Which NTIA Could Focus Funding and Resources, such as Through Private Test Labs.

With O-RAN Alliance specifications developed for the Central Units ("CU"), Distributed Units ("DU"), and Radio Units ("RU"), interoperability is a major piece of the Open RAN

[40] TelecomTV, *Vodafone and NTT DOCOMO sign MoU to cooperate to drive greater system integration and service efficiency in Open RAN* (Oct. 25, 2022), https://www.telecomtv.com/content/open-ran/vodafone-and-ntt-docomo-sign-mou-to-cooperate-to-drive-greater-system-integration-and-service-efficiency-in-open-ran-45765/.

puzzle. NTIA has recognized this and taken concrete steps to address it, in work like its 5G Challenge which kicked off in 2022 and will expand in 2023.[41] NTIA could build on this work and use the Innovation Fund to promote interoperability efforts.

More specifically, NTIA could use the Innovation Fund to support open interoperability multi-vendor labs accessible to vendors in the private sector. Interoperability labs would allow smaller organizations to avoid capital expenditures to build their own testing facilities. Trusted labs would also reduce costs for operators, since they would not need to pay for individual testing. Labs would test interoperability among Open RAN RU, DU, and CU components.[42] NTIA could aim to have these labs become qualified Open Testing and Integration Centres ("OTIC") with the O-RAN Alliance.[43] NTIA funding to labs could help build network operator confidence and trust in Open RAN solutions offered by suppliers.

Additionally, NTIA could fund plugfests. NTIA asks if interoperability and debugging events—usually called "plugfests"[44]—are effective mechanisms to support Open RAN equipment interoperability.[45] Suppliers are currently engaging in plugfests to test interoperability during product development. If NTIA assumed some of the costs of plugfests, it could open up resources to focus on other interoperability solutions.

D. NTIA Could Fund Industry-led, Third Party Certification of Equipment to O-RAN Alliance Specifications.

[41] NTIA, *5G Challenge*, https://5gchallenge.ntia.gov/ (last accessed Jan. 24, 2023).

[42] *See* O-RAN Alliance, *O-Ran Architecture Overview*, https://docs.o-ran-sc.org/en/latest/architecture/architecture.html (last accessed Jan. 24, 2023).

[43] *See* O-RAN Alliance, *Testing & Integration*, https://www.o-ran.org/testing-integration.

[44] *See* O-RAN Alliance, *PlugFests and Proofs of Concept*, https://www.o-ran.org/testing-integration#plugfests-and-proof (last accessed Jan. 24, 2023).

[45] RFC 9(a).

NTIA seeks input on several certification-related issues. The RFC asks, "How do certification programs impact commercial adoption and deployment?"[46] The RFC also asks about whether certification programs would be necessary for a "successful marketplace" as well as what "bodies or fora" would host such a certification process, among other questions.[47]

The private sector is addressing Open RAN testing and certification, but NTIA could support additional resources to get equipment certified so that smaller operators and private networks can identify suitable equipment. When it comes to compliance, the O-RAN Alliance functions as a specification body and 3GPP does not produce standards related to RAN systems. The O-RAN Alliance does not engage in certification. Instead, testing for compliance with O-RAN Alliance specifications takes place individually by providers in their own labs.

Similar to labs that test interoperability, NTIA could fund private labs that ensure that vendor Open RAN equipment complies with O-RAN Alliance specifications, but a formal certification process may introduce tradeoffs. These third-party labs could provide similar benefits as any interoperability labs, assisting smaller providers and operators alike by decreasing the expenditures needed for internal standards compliance testing. Labs could also provide recertification as new specifications are released. The FCC's CSRIC has explained that a certification process could reduce integration time between multiple vendors and show compliance to interoperability and security standards.[48] However, CSRIC has also qualified these benefits, explaining that "A formal certification process has many tradeoffs that could either hurt or benefit potential stakeholders, including national operators, rural operators, large vendors, small vendors, and government agencies. Independent of the certification process,

[46] RFC 11.

[47] RFC 11-12.

[48] CSRIC Open RAN Report at 44.

stakeholders are recommended to apply the O-RAN Alliance's test specifications as applicable."[49] NTIA should consider weighing tradeoffs if it chooses to pursue the funding of private labs to create an industry-led, third-party certification process.

Although NTIA could fund private labs, the agency should avoid creating redundancy or duplicative testing requirements if it chooses to promote any Open RAN certification regime or process. Equipment vendors tend to test equipment in coordination with the network provider that will utilize the equipment. This equipment is tested to ensure that it meets the provider's standards. *Requiring* independent Open RAN standards certification through an additional party could create redundant testing, since the vendor would still have to test with the provider. NTIA should avoid creating any duplicative certification requirements as it continues to draft NOFOs. Importantly, if NTIA were to establish any industry-led certification processes, operators should be free to choose whether to require such certification. This would be consistent with GSMA's Network Equipment Security Assurance Scheme, for example.[50]

V. NTIA SHOULD SUPPORT TEST BEDS AND PILOT PROGRAMS, HEEDING CONGRESSIONAL DIRECTION TO SUPPORT INNOVATION WITHOUT DUPLICATING EXISTING WORK.

The RFC asks several questions about the use of test beds and pilot programs to further the goals of the Innovation Fund.[51]

A. Test Beds, Like the Wireless 5G Security Test Bed, Can Promote Development of Open RAN Technology and Help Address Challenges in Interoperability, System Integration, and Security.

[49] *Id.*

[50] GSMA, *GSMA Network Equipment Security Assurance Scheme (NESAS)*, https://www.gsma.com/security/network-equipment-security-assurance-scheme/ (last accessed Jan. 24, 2023).

[51] RFC 14-15.

Congress contemplated NTIA support for test beds and collaborative R&D. In Section 906, Congress directed NTIA to avoid duplication of existing research.[52] There may be test beds that can be leveraged, funded, or created to benefit from the Innovation Fund and focus on interoperability and other challenges.[53]

Existing test beds can also address security issues in Open RAN. The RFC asks several questions about security in Open RAN.[54] NTIA should consider CTIA's 5G Security Test Bed as it shapes funding opportunities.[55] Currently, 5G is the most secure generation of wireless to date. As numerous government groups focus on understanding and assessing the 5G landscape, CTIA launched its 5G Security Test Bed to provide these groups, as well as the wireless and technology industries generally, a real-world, practical environment to test recommendations and security solutions. The 5G Security Testbed will be an available venue for novel, Open RAN-specific programs supported by the Innovation Fund. These programs could test Open RAN security practices, such as those recommended in CSRIC VIII's recent Open RAN Report.[56]

B. NTIA Might Consider How Pilot Programs Could Help Smaller Carriers or Private Networks Move Toward Open RAN by Addressing Interoperability and Scale Challenges.

[52] *See* 47 U.S.C. § 906(a)(1)(D).

[53] *See, e.g.*, Press Release, Nokia, Nokia partners with Hill Air Force Base on testbed for radar interference management with Open RAN architecture (July 12, 2022), https://www.nokia.com/about-us/news/releases/2022/07/12/nokia-partners-with-hill-air-force-base-on-testbed-for-radar-interference-management-with-open-ran-architecture/; Commonwealth Cyber Initiative, *CCI xG Testbed Leads O-RAN Research*, https://cyberinitiative.org/xg-testbed/cci-xg-testbed-leads-way-in-end-to-end-o-ran.html (last accessed Jan. 24, 2023); Press Release, Mavenir and Northeastern University Announce the Availability of Open-Source Open RAN Simulation Platform (Oct. 11, 2022), https://www.mavenir.com/press-releases/mavenir-and-northeastern-university-announce-the-availability-of-open-source-open-ran-simulation-platform/.

[54] RFC 17(a)-(b), 19.

[55] 5G Security Test Bed Information Sheet, available at https://5gsecuritytestbed.com/wp-content/uploads/2022/06/STB-One-Pager_061422.pdf (last accessed Jan. 24, 2023).

[56] *See generally* CSRIC Open RAN Report.

NTIA could consider funding specialized pilot programs that could provide benefits to the larger communications community. While NTIA should generally not use the Innovation Fund to subsidize equipment purchases or other Open RAN deployments by carriers, there may be value in helping universities or enterprises move to Open RAN in private networks or smaller deployments where some challenges around system integration can be tackled and resolved. NTIA could condition any such funding for deployments on a commitment to share experiences and lessons learned with NTIA and the public. This may help refine approaches and provide models for transition to Open RAN deployments as well as small form factor and power efficient deployments.

VI. NTIA COULD PROVIDE INCENTIVES FOR OTHER OPEN RAN EFFORTS, SUCH AS PNT OPEN RAN PROJECTS.

There are discrete projects that NTIA could consider for eligibility as it shapes NOFOs, from advancing innovation in position, navigation, and timing ("PNT") solutions in Open RAN settings to energy efficiency.

In the area of PNT, NTIA could fund projects to establish comprehensive and resilient national timing architecture based on Universal Coordinated Time ("UTC"). A national timing architecture will assist with Open RAN deployment. RAN and Open RAN transmitters and receivers need timing for server virtualization, antenna synchronization, and frequency discipline. Additionally, disaggregation in Open RAN makes reliance on clock holdover with high stability oscillators less feasible.[57] The O-RAN Alliance is currently addressing standards for timing, and it has developed a third version of its *Synchronization Architecture and Solution*

[57] *See, e.g.*, Jim Olsen, *Meet timing requirements in 5G networks*, 5G Technology World (May 31, 2021), https://www.5gtechnologyworld.com/meet-timing-requirements-in-5g-networks/.

Specification.[58] The International Telecommunication Union recently noted that RANs and 5G rely on precise timing and synchronization.[59]

NTIA funding could support U.S. innovation and leadership in PNT. The federal government outlined the characteristics of a national PNT architecture in a 2008 report[60] and has since prioritized several PNT workstreams to address resilience and security,[61] in which CTIA has been pleased to participate. In the 2008 report, the government made recommendations for a national PNT architecture and "US leadership in global PNT."[62] While the 2008 report may be outdated, the principles and characteristics needed in a national PNT or timing architecture outlined therein remain relevant. A resilient national timing architecture will increase access to multi-source, reliable time and synchronization. More accessible and synchronized national timing will allow for operational efficiencies and more American innovation. A competitive PNT architecture would be able to support certain 5G and Open RAN deployments.

In addition to PNT, CTIA identifies further efforts that NTIA could promote as it implements the Innovation Fund. NTIA could promote:

- Projects that support hardware design and energy efficiency. NTIA could promote projects that support the development of hardware reference designs that have small form factor and better energy efficiency. These projects are particularly important for small cell deployments. Specifically, these projects could support Open RAN RU vendors and radio frequency ("RF") component manufacturers.
- R&D of Non-Real Time ("RT") RAN Intelligent Controller ("RIC") and Near RT RIC applications that comply with O-RAN Alliance RIC specifications.

[58] O-RAN Alliance, O-RAN Synchronization Architecture and Solution Specification 3.0 (Oct. 2022), available at https://orandownloadsweb.azurewebsites.net/specifications (last accessed Jan. 24, 2023).

[59] ITU, *Synchronization technologies evolving for 5G and beyond* (Dec. 20, 2022), https://www.itu.int/hub/2022/12/synchronization-technologies-evolving-for-5g-and-beyond/.

[60] National Security Space Office, National Positioning, Navigation, and Timing Architecture Study, Final Report (Sept. 2008), available at https://rosap.ntl.bts.gov/view/dot/34816 (last accessed Jan. 23, 2023).

[61] *See, e.g.*, Executive Order 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services, 85 Fed. Reg. 9,359 (Feb. 12, 2020).

[62] *Id.* at 86.

- Over-the-air Open RAN RU outdoor antenna test ranges to help test different suppliers' Open RAN RU solutions.
- Making Open RAN equipment eligible for rural deployment.

These efforts could help promote Open RAN deployments across more varied use cases.

VII. CONCLUSION

CTIA supports federal promotion of Open RAN, where such support or any NOFOs do not provide rigid requirements and provide flexibility to grantees, to best promote Open RAN deployments. CTIA looks forward to further collaboration with NTIA as it begins to implement the Innovation Fund.

Respectfully submitted,

/s/ *Thomas C. Power*
Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

January 27, 2023