ITI Promoting Innovation Worldwide

January 27, 2023

ITI Comments
NTIA's Public Wireless Supply Chain Innovation Fund

Introduction

ITI appreciates the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) Request for Comment on the Public Wireless Supply Chain Innovation Fund Implementation (Innovation Fund). We believe this grant program will be useful to advance USG objectives related to the deployment of open and interoperable, standards-based radio access networks.

ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. ITI's diverse membership comprises companies that operate in almost every layer of the 5G stack, including semiconductor and network equipment designers and manufacturers, software, and digital services companies, as well as those that will harness 5G and NextG to evolve their businesses.

We have supported the USG's increased focus on enabling the deployment of the next generation of cellular network technology; indeed, 5G will be transformative for our society, offering opportunities to companies and consumers not previously available. In particular, we were supportive of the previous Administration's efforts to develop a whole-of-government approach to 5G in its *National Strategy to Secure 5G* and Implementation Plan and its focus on promoting the secure development and deployment of 5G globally, with one activity in particular aimed at developing policies and strategies for global market competitiveness and diversity. We appreciate that the RFC references the *National Strategy to Secure 5G Implementation Plan* in the questions related to security and encourage NTIA to more explicitly detail how the Innovation Fund will support this activity as it develops guidance to administer the program. Open and interoperable standards-based Radio Access Networks (RAN) can increase innovation and bolster competitiveness by allowing for flexibility and facilitating the entry of new market participants and so helps to support that specific activity. At the same time, we reiterate that this is only *one* activity that will help to promote the deployment of secure 5G and the need for a holistic approach remains paramount.

The US is leading the way on Open RAN with one of the world's first large-scale Open RAN network currently being deployed. However, just like any new technology, hurdles remain related to Open RAN's development, deployment, and adoption. Specifically, our member companies have identified challenges in multi-vendor interoperability, end-to-end system integration, and workforce readiness. NTIA's Innovation Fund can help address these issues by complementing the ongoing work in the private sector.

Focus on domestic public-private partnerships can drive all relevant players to collaborate on specific 5G/6G innovation, including operators, end users, system integrators, colleges and technology companies jointly implementing specific forward looking use cases. Funding for public labs hosting debugging events, 'plugfests' or other interoperability testing will help new entrants demonstrate viability along the stack, while pairing government funding with already existing research and development projects in the private sector can identify compelling Open RAN use cases and ensure that the technologies developed serve operator needs. Finally, as

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

network operators transform their networks, they are concurrently transforming their workforces to ensure smooth deployment and maintenance of virtualized infrastructure.

Below, we offer thoughts on several questions posed in the RFC. Our responses are not exhaustive but focus on those that are most relevant to our membership.

As such our top-line recommendations include:

- Focus on pilots and commercial deployments to further advance end-to-end real-world testing
- Include foundational cybersecurity criteria, e.g. adhering to cyber standards/best practices and enabling security architectures, as a pre-requisite for grant funding
- Disburse awards quickly to support new projects and start ups
- Do not limit awards to only companies headquartered in the US

Questions the on the State of the Industry

1. What are the chief challenges to the adoption and deployment of open and interoperable, standards-based RAN, such as Open RAN? Are those challenges different for public vs. private networks? a. What are the challenges for brownfield deployments, in which existing networks are upgraded to incorporate open, interoperable, and standards-based equipment?

There are now commercial scale deployments of mobile networks utilizing Open-RAN in a green field environment, including the DISH 5G network, which is cloud-native and operates on an Open-RAN-based infrastructure. As of June 2022, DISH's 5G network was deployed and commercially available to more than 20% of the US population. These deployments show that Open-RAN is no longer in its infancy and to continue prodding the technology, NTIA can focus on pilot projects and commercial deployments.

That is not to say there are not still difficulties when it comes to integration generally and in brownfield deployments. Network operators will likely bear the burden of integration. There is not single point of responsibility which adds to the accountability, oversight, cost and management burden for operators. On the other hand, with an open architecture, there is more visibility at every layer and within each of the interface points within each vendor so management can be more effective in that sense. Private networks also need to contend with these challenges albeit at a much lower scale, performance, and complexity. The lower scale of private networks may allow early opportunities for Open RAN success. NTIA support for end-to-end testing in commercial environments can assist in alleviating some of the difficulties involved when it comes to network integration and other transitions.

Regardless of difficulties, it remains vital to the US and its national security interests to spur the development of this market particularly in technical areas of risk from multivendor, interoperable, standards-based deployments.

2. What ongoing public and private sector initiatives may be relevant to the Innovation Fund?

There are several key initiatives that NTIA could be interacting with, in a variety of possible ways ranging from consulting on topics of interest, to engaging as a partner in executing on projects. A few that stand out to us are:

The ATIS NextG Alliance is an initiative to advance North American mobile technology leadership in the next decade. NGA has a wide representation within the private and public sectors and includes some 100 companies, government agencies, academic institutions etc. from North America.

NSF plays a pivotal role in funding wireless research and partnering with the mobile industry, and here we highlight some key activities. Its new TIP directorate aims to accelerate translational research that will drive tomorrow's technologies and solutions. Wireless is among the prioritized topics of TIP. The RINGS program is a public private partnership with 9 industry leaders, and funding some 40 projects, aimed at the development of intelligent, resilient, and reliable next generation networks. The PAWR program supports 4 large wireless research testbeds. It is funded by a partnership of NSF and a consortium of 30 companies. The Convergence Accelerator program runs yearly cohorts of small teams through a process from ideation to societal impact. Its 2022 cohort includes a track on Securely Operating Through 5G Infrastructure. We can expect NSF to lead more programs of high relevance going forward.

SRC JUMP 2.0 is a large program in cooperation with DARPA focused on the performance, efficiency, and capabilities of broad classes of electronics systems for both commercial and military applications. Several of its themes are highly relevant to mobile networks, including Communications and Connectivity, Cognition, and Intelligent Sensing to Action.

4. What is the current climate for private investment in Open RAN, and how can the Innovation Fund help increase and accelerate the pace of investment by public and private entities?

In our answers to questions 6-16, we suggest several options that NTIA might consider, including expanding on existing projects, funding a new public lab, and disbursing awards to pilot projects, commercial trials, radio and App development and end-to-end environments. These are however steppingstones to enabling broader adoption of Open-RAN on a competitive timeline. Funds should be focused on projects that will mature the technology and scale it to meet the challenges for network operators and broader commercial deployment.

Questions on Technology Development and Standards (Questions 6-8)

NTIA asks about the current state of open and interoperable, standards-based RAN, the readiness of standards and how to prepare for future technological generations. NTIA should continue to follow industry's lead and support equipment developed pursuant to the standards set forth by organizations such as the O-RAN Alliance, the Telecom Infra Project, 3GPP, the O-RAN Software Community, or any successor organizations.

These organizations have developed mature specifications that build on legacy technologies and components. These established industry groups and organizations are not reinventing the wheel. Each group is dedicated to defining various attributes for open interfaces, aligning on those interfaces and publishing agreed specifications. As a result, these global standards can be relied on to ensure network performance, scalability and architecture interoperability. In this way we would say much of the maturation process at this time is in some instances testing and commercial/pilot deployments.

To support the industry's continued growth, NTIA should promote Open RAN success stories both domestically and internationally to highlight the viability of 5G networks built with Open RAN standards. For example, supporting global 5G standards or technical specifications rather than promoting or mandating country-specific standards will prevent the development of a balkanized system resulting in varying national requirements. As

standards continue to develop, NTIA should encourage the use of open-source software and existing specifications to increase the velocity of ORAN adoption. We believe that the NTIA, as a part of broader U.S. policy, should expressly advance a diverse, trusted market of suppliers based in the United States as well as in allied and other partner market democracies. Only a multinational, diverse vendor base of trusted suppliers will have the capacity to service the U.S. and other partner countries' markets.

NextG technologies and O-RAN specifically will require interoperability of products to reach feasible scale and realize the value of mobile connectivity. This means that NTIA and USG broadly also should support industries' – and all companies' – full participation in international standards development bodies. A harmonized international system depends on the contributions and participation of all relevant stakeholders, including governments, to develop standards that are most appropriate for the market and current technology.

International standards enable products to operate across markets, meet consumer needs, support implementation of strong security measures, and drive economic opportunity for every sector of the economy. Governments and the private sector alike must protect and promote international standards and the rules-based processes that enable consensus-based, industry-driven development of technical standards. Standards and specification development processes have built-in rules and safeguards that prevent any actor from singlehandedly exerting inappropriate influence on a standard. These rules and processes also support transparency of technical elements that is essential for trust of any system. As a means to protect and promote this rules-based system, governments should avoid taking a top-down approach and should encourage consistent industry engagement, without directing or controlling industry's activities.

Policymakers should encourage consistent industry engagement in international standards activities. Consistent engagement in international standards development organizations is crucial to understanding the system, developing influence, and effectively competing and cooperating with other companies and stakeholders to harmonize technical standards for the benefits of citizens and industry alike. It is also essential to the value of transparent processes that technical standards are reviewed by qualified experts. Governments should also consistently engage in international standards development activities as appropriate.

Questions on Integration, Interoperability, and Certification (Questions 9-12)

As NTIA notes in the Request for Comment, "[c]hallenges associated with systems integration and component interoperability can hinder the adoption of open and interoperable, standards-based RAN." Certain supply chain inefficiencies have arisen from a disaggregated, multi-vendor approach to systems that historically have been closed and controlled by a single vendor. In the current disaggregated environment, every operator must perform end-to-end validation of the full RAN system. This approach is both costly and generally limited to the use of a few incumbent vendors and individual operators. As a result, the adoption of Open RAN to date remains limited.

Effectively and sustainably solving this challenge requires coordination across the industry. The most efficient solution would be for industry to align on a system, platform, or framework that helps coordinate the entire roadmap and lifecycle process, from the pooling of requirements at an industry level to establishing a "marketplace" of commercial-ready products and solutions and creates a system release validation and certification process. NTIA should support proposals that take (or support) such a holistic approach, so that duplicated efforts can be minimized across hundreds of operators and their vendors. Without such a process, the difficulty and complexity of integration could continue to outweigh the benefits of disaggregation and Open RAN

will not achieve the economies of scale needed to be a viable alternative to incumbent systems in time for the 6G development cycle.

There are many aspects that will contribute to the success of 5G and NextG networks. While some will be green field deployments demonstrating use cases, the speed of technological transitions of legacy telecom operators is a key component to success. The transition to Open RAN in many ways is similar to the transition from local to cloud computing.

As such, the Innovation Fund can support projects that focus on end-to-end interoperability and debugging events, or "plugfests," where different vendors can bring their software, verify, and fine tune interoperability with other components. These types of events allow operators more certainty for deployments in real world scenarios and during technology transitions. NTIA can support the creation of an interoperability blueprint and testing facilities, accessible by all vendors, regardless of size and revenue. As mentioned above, Open RAN is already being deployed in the U.S. NTIA's support for end-to-end interoperability testing environments will complement ongoing private sector efforts. This support would contribute towards building robust Open RAN ecosystems by helping vendors create deployment and maintenance tools and explore vertical use cases.

Questions on Trials, Pilots, Use Cases, and Market Development (Qs 13-16)

As the Request for Comment rightly notes that the "key aim of the Innovation Fund is to promote and deploy technologies that will enhance competitiveness of 5G and successor open and interoperable, standards-based RAN." We would suggest that NTIA focus on deployment in the form of pilot projects, commercial deployments, and opportunities for end-to-end integration testing.

13. What are the foreseeable use cases for open and interoperable, standards-based networks, such as Open RAN, including for public and private 5G networks?

While 5G connectivity is the beginning of many sector-specific capabilities, open networking technologies will continue to allow for additional agility in network slicing, spectrum sharing, and computing power required for enhanced robotics and AI/ML.

NTIA may want to take notice of projects focused on the RAN Intelligent Controller (RIC) platform. The RIC is a platform that is used to control and manage the mobile Radio Access Network and provides a centralized, programmable interface for managing the RAN and enables real-time, fine-grained control of the network. It can use AI/ML algorithms to optimize network performance. The RIC is typically implemented as a software solution that runs on servers or virtual machines in a cloud or data center environment making it a ripe environment for app developers looking to develop intelligent functions for the RAN.

This can include xApp features such as dynamic resource allocation, self-organizing network (SON) capabilities, and network slicing or rApp features that include interference, mobility, and quality of service management. As these are cloud native functions and can run anywhere on the network from the core to the edge it is possible for communications service providers to move intelligence away from the cell site and throughout the network. As such, NTIA can consider funding projects that include AI/ML, edge computing, network management and security.

14. What kinds of trials, use cases, feasibility studies, or proofs of concept will help achieve the goals identified in 47 U.S.C. 906(a)(1)(C), including accelerating commercial deployments?

As we will detail below, there are already a number of testbeds in existence and while there may be some opportunities in this space particularly to iron out challenges around integration, NTIA may find the most effective way to encourage the industry is by focusing funding on pilot projects and commercial deployments.

Industry will not deploy Open RAN for Open RAN's sake. The movement to develop Open RAN was led by carriers looking to spur greater supply chain diversification through the use of open, interoperable standards that can lower barriers to entry, drive adoption of innovations, and leverage more cost-efficient technologies anchored in software, cloud, and virtualization. At the same time, their customers and regulators are exacting in their expectations for network reliability and resilience. Pilots, plug fests, proofs of concept, testbeds, and small-scale deployments are steppingstones to addressing those concerns and enabling broader adoption of Open RAN on a timeline relevant to 5G. NTIA should therefore focus funds into areas that will mature the technology and scale it to meet the challenges for network operators and other commercial deployments.

In the public sector, it may make sense for NTIA to support a new lab or expand on existing Innovation Zones. For example, funding a federated lab system facilitated by a neutral third- party coordinator could help leverage existing facilities in a way that makes them more accessible to participants. These types of environments can support the ecosystem development and research particularly in performance advancements and research for what 6G will entail. Long term lifecycles can make the telecom industry particularly challenging for maintaining presence in the long term. Neutral research environments that can be repurposed as some of the Innovation Zones have been, can support the industry through a lifecycle "dip" into the next stage of innovation

Additionally, further end-to-end pilots/testing on security will lead to more reliable infrastructure at the outset. For example, having additional security test beds that examine security scenarios identified through bodies such as the CSRIC at the FCC or findings from the Enduring Security Framework allow industry to work on and test recommendations or identify other threat scenarios. Once items that need to be addressed have been identified, standards can be developed and brought back to industry led standards bodies, such as 3GPP. Publicly accessible test beds will allow for new entrants to participate in various scenarios. Testing Labs can be designed for penetration tests on the products that include a bug-bounty program for issues found. From lessons learned private and/or public testing labs can setup a way for O-RAN vendors and suppliers to share threat intelligence before and after deployments.

15. How might existing testbeds be utilized to accelerate adoption and deployment?

NTIA could extend the approaches taken in innovation zones in New York and Salt Lake City adapted for 5G/open RAN to more locations. A similar initiative exists in the UK, where the Digital Catapult runs a project called SONIC, focused on ORAN interoperability. Existing interoperability labs could also be extended to cover the Open RAN use case: for example, the University of New Hampshire Interoperability Laboratory (UNH-IOL). An open 5G testbed, with dedicated staff and technical infrastructure, that can enable participants to test their Open RAN components on an open cloud infrastructure using commercial off-the-shelf hardware will bring more players to the table.

In that vein, in November 2021, the Federal Communications Commission created two new Innovation Zones for Program Experimental Licenses in designated areas near North Carolina State University (NC State Innovation Zone) in Raleigh, NC and Northeastern University (Northeastern Innovation Zone) in Boston, MA and expanded the Innovation Zone near New York city. The AERPAW—Aerial Experimentation and Research Platform for Advanced Wireless in Raleigh, North Carolina is working on a city-scale testbed focusing on solutions in various unmanned aerial system verticals including beyond visual line-of-sight. The testbed is also able to provide verification, and testing of other possibilities in telecommunications, transportation, infrastructure monitoring,

agriculture, and public safety. At Northeastern University in Boston, Massachusetts, the testbed can emulate full-stack communications, and support artificial intelligence and machine learning algorithms and hardware in the loop to accelerate advancements in wireless networked systems including Open RAN.

The existing Innovation Zone testbeds are allowing for specific use case testing. Testbeds and demonstration projects that can help small and large firms alike identify and solve challenges related to the performance of Open RAN technology facilitate the development of new use cases, and further "de-risk" the technology. At this time, a best focus for the NTIA PWSCIF is likely funding the real-world deployments of projects that have already demonstrated value in testing. Real-world end-to-end validation projects could be a key area for NTIA to focus as many operators remain concerned about integration.

Questions on Security (17-20)

Below, we offer thoughts on the overarching questions NTIA poses in its RFC on security related to open and interoperable standards-based RAN:

17. "Promoting and deploying security features enhancing the integrity and availability of equipment in multi-vendor networks," is a key aim of the Innovation Fund (47 U.S.C 906(a)(1)(C)(vi)). How can the projects and initiatives funded through the program best address this goal and alleviate some of the ongoing concerns relating to the security of open and interoperable, standards-based RAN?

As a general matter, we believe that the criteria related to receiving grants from the Innovation Fund should incorporate security. While companies are already taking steps to improve the security of open and interoperable, standards-based deployments, such an approach will further incentivize good cybersecurity practices. We also believe that the promise of open and interoperable, standards-based RAN can be most fully realized through enterprise-grade security - which means the ability to secure the service, hardware, software, technology, and application stack by securing all layers (hardware, signaling, data, applications and management), all locations, all attack vectors, and all hardware and software life cycle stages. It is foundational to enable organizations to take a zero-trust approach to their multi-vendor networks, including applying security on the network slice level. The projects and initiatives funded through the program should recognize these principles as foundational security elements to build upon and mature use cases around.

a. *What role should security reporting play in the program's criteria?*

The RFC asks what role security reporting should play in the program's criteria. We encourage NTIA to further explain what it means by security reporting – is it talking about security incident notification or is it talking about security benchmarks reporting and risk analysis scorecards?

We note that critical infrastructure owners and operators are already subject to mandatory security incident reporting requirements under the Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 and that there is a plethora of other federal regimes in place that require the reporting of security incidents. The Cybersecurity and Infrastructure Security Agency (CISA) is still in the process of determining what constitutes a 'covered entity' under that rulemaking, so we encourage NTIA to wait to see the outcome of that process before instituting additional requirements, as companies applying for grants from the Innovation Fund may already be subject to mandatory requirements under CIRICA. Under CIRCIA, these reporting and coordinated vulnerability

disclosure requirements should be further aligned on international standards and industry best practices (compare also to the IoT Cybersecurity Improvement Act).

However, if by security reporting NTIA means security benchmarks and risk analysis scorecards, funding could be applied for the United States to establish security parameters and benchmarks in coordination with key security organizations, which could then be standardized at the O-RAN Alliance. There is presently a gap in defined security parameters and/or benchmarks to help determine success or failure.

b. *What role should security elements or requirements, such as industry standards, best practices, and frameworks, play in the program's criteria?*

Security elements should play a key role in the program's criteria. We encourage adherence to consensus-based international cybersecurity standards, reference designs, best practices, and mobile security patents, consistent 3GPP to be included as a foundational requirement to receive grant funding. For example, frameworks such as the MITRE FiGHT 5G Framework may be useful to incorporate in criteria so as to have a common definition and database of vulnerabilities, threats and TTPs related to 5G Networks. The framework has done this incredibly well for general IT networks and the same needs to be supported in mobile networks now that these networks are beginning to open up.

Companies should attest that they are adhering to such standards.

18. What steps are companies already taking to address security concerns?

While O-RAN architecture can create an expanded threat surface[1], work is currently underway to ensure the security of additional O-RAN interfaces and functions. Indeed, companies are already taking steps to address security concerns, both internally and as a part of standards groups. For example, several of our member companies are a part of the O-RAN Alliance, which formed a Security Focus Group in 2020. The SFG is advising O-RAN Working Groups to evolve their standards to make O-RAN specific architectural changes more secure in order to meet the expectations of network operators and their customers. The SFG has produced several technical specifications related to security testing, protocols, and requirements, which companies can leverage to ensure that O-RAN deployments are as secure as proprietary deployments.[2] It is also continuing progress on work items aimed at better securing the O-RAN Open Fronthaul Interface, Near-Real-Time Radio Intelligent Controller (Near-RT RIC) and third-party xApps, and the SMO Non-Real-Time RIC. The group is also working on updating the O-RAN risk analysis with likelihood scores.[3]

Although virtualization increases the threat surface, open RAN-based architectures that incorporate virtualization can also provide opportunity for building increased security features into the network. A core component of 5G is the cloud-native fabric. This allows for additional security enhancements and capabilities. For example, it facilitates the rapid deployment of infrastructure and services. This is done via incorporating leading security practices and standards into the development lifecycles to address operator requirements, integrating zero-trust architecture, and using cloud services as a catalyst to further security innovation, employing IoT, big data, and AI/ML. It also allows for greater visibility into threats and security telemetry, while facilitating a scalable and

[1] See CSRIC VIII Report here, which outlines security concerns and recommendations to address O-RAN security: https://www.fcc.gov/file/24520/download as well as Enduring Security Framework report on Open Radio Access Network Security Considerations here: https://www.cisa.gov/blog/2022/09/15/securing-5g-open-ran-architecture-cybersecurity-risks
[2] https://www.o-ran.org/blog/the-o-ran-alliance-security-focus-group-progresses-in-defining-o-ran-security-solutions
[3] Ibid.

dynamic approach. Networks built on open and interoperable standards, in particular, allow for greater transparency into the lifecycle process.[4]

Security capabilities and services are continuously created and deployed to secure cloud architecture. Ultimately centered around a zero-trust approach and a secure development lifecycle, cloud security capabilities are distributed across the lifecycle, including during the "build" stage, when developers are pushing code into the cloud, as well as during the operations and maintenance stage. Cloud security uses practices that support security assurance and compliance requirements across the entire lifecycle of these services. This helps operators and enterprises alike build highly secure software, address security compliance requirements through automation, and reduce development and deployment costs. It also includes elements such as vulnerability management processes to periodically scan and validate services. Leveraging cloud-native services also unlocks automated security compliance capabilities across the product lifecycle from procurement to sunsetting to support operators. Finally, cloud capabilities also deliver enhanced platform security by integrating NIST SP 800-193 – Platform Firmware Resiliency Guidelines into 5G edge deployment.

19. What role can the Innovation Fund play in strengthening the security of open and interoperable, standards-based RAN?

By instituting conditions related to grant funding that are specific to security, the Innovation Fund can at a minimum incentivize potential recipients to ensure that they are meeting foundational cybersecurity requirements.

We also reference earlier in our response the importance of testbeds for security (see response to question 15). The Innovation Fund, by supporting the continued creation of such testbeds, can help to inform recommendations related to security scenarios, including by identifying what specific technical specifications may be required to mitigate discovered risks.

Overall, it is important to note that several of the security concerns that have been identified with regard to Open RAN are also applicable to 5G/NextG network architecture more broadly. Indeed, the use of virtualization is not specific to Open RAN. With that being said, we do not believe that funding should be used in an attempt to solve these broader security concerns related to the use of virtualization but should instead be more targeted. In our view, security concerns worth addressing with these funds are those specific to multivendor deployments and the interoperability required to achieve that vision.

20. 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?

See above answer to question 18, where we discuss how the zero-trust approach is incorporated into network deployment. Indeed, given the increasing emphasis on virtualization in the deployment of 5G, the zero-trust approach is a building block for security. Additionally, as we reference above, the O-RAN Alliance SFG is updating its risk analysis scores and is particularly considering the Zero Trust Architecture published by NIST (SP 800-207) to ensure that potential impacts and likelihood of risks is appropriately quantified.

[4] Please see our prior submission to the FCC responding to an NOI on *Promoting the Deployment of 5G Open Radio Access Networks* for more information: https://www.itic.org/documents/emerging-technologies/ITIResponsetoFCCOpenRANNOI-FINAL.pdf

Program Execution and Collaboration

The RFC requests feedback on how program requirements and monitoring can be tailored to achieve its goals. *22. How can NTIA ensure that a diverse array of stakeholders can compete for funding? 23. How, if at all, should NTIA promote teaming and/or encourage industry consortiums to apply for grants? And 24. How can NTIA maximize matching contributions by entities seeking grants without adversely discouraging participation?*
We would like to express that it is very important for NTIA to move quickly on its grant disbursement process to ensure the highest level of participation from possible awardees.

Teaming should be allowed. Entities working together to develop end-to-end solutions, commercial pilots or deployments may present efficiencies to move the technology life-cycle forward. The ability to pair private funds with government dollars should be considered but should not be dispositive. As supplier diversity is a primary goal of the fund, smaller entities, start-ups, and new App developers should receive the same consideration as others.
25. How can the fund ensure that programs promote U.S. competitiveness in the 5G market?
Boosting US competitiveness in the 5G market is critical, and there are multiple policy avenues that support this.

However, we note that applying Build America, Buy America (BABA) or similar domestic sourcing requirements to innovation fund grants would not support U.S. competitiveness in the 5G market. According to a report issued by the Information Technology and Innovation Foundation (ITIF), applying Buy America requirements to the technologies needed to fulfill broadband and other infrastructure projects will ultimately increase IT costs by 25 percent.[5] Depending on where the products are sourced, the cost increase for some would be more than 25 percent. Moreover, applying BABA provisions, even if significant case-by-case waivers are allowed, would increase regulatory complexity and costs, meaning fewer projects can be completed. Finally, because the production of 5G technology is complex, it is extremely difficult to quickly create domestic production capabilities. This means that applying BABA to 5G technology provided as part of innovation fund projects will significantly delay project completion until domestic production can be created. Otherwise, projects will have to use older, lower-quality domestic technology.

Many of ITI's member companies – and countless companies across the United States – rely on globally-sourced materials to develop and manufacture the innovative end products that power U.S. national security and technical innovation, including supporting the day-to-day operation of the U.S Government. Additionally, virtually all our member companies rely on products that contain globally sourced materials for carrying out their business activities. As such, applying Buy America requirements to innovation fund grants will not incentivize the domestic production of 5G or improve the United States' competitiveness globally. Rather, applying strict BABA requirements to innovation fund projects will negatively impact competition, supplier diversity, supply chain resiliency, and opportunities for small and disadvantaged businesses to participate in government business opportunities and the larger global 5G market.

In short, applying Buy America requirements to the development of 5G technologies may interfere with competitiveness of American contractors at home and abroad. If a contractor bids on a project using potentially more expensive American-made products, they will likely assume their competitors' bids include the same costs. If American products turn out to be substantially greater in cost, the contractor that uses them will be less competitive in other bidding opportunities. Likewise, these restrictions will risk interfering with the competitiveness of American contractors abroad. Preferential treatment for American-made products on U.S. soil will encourage reciprocal action abroad. Contractors who do business overseas could lose business on foreign government or commercial projects for which they otherwise would have been competitive.

[5] https://itif.org/publications/2022/05/09/how-applying-buy-america-provisions-it-undermines-infrastructure-goals/

a. *Should NTIA require that grantee projects take place in the U.S.?*

The Congressional intent of this fund is to develop supplier diversity domestically, but that does not mean that our trusted international partners should be precluded from participating in the fund on domestic projects. U.S. policy should not focus narrowly on U.S.-headquartered companies or the U.S. market alone. Instead, policymakers should promote a diverse, competitive ecosystem of suppliers headquartered in the U.S. and partner countries that collectively have the capacity to serve the growing needs of U.S. carriers and the 5G market. Our trusted partners have large scale operations in the United States and provide a significant number of US jobs. All promising projects should be considered.

b. *How should NTIA address potential grantees based in the U.S. with significant overseas operations and potential grantees not based in the U.S. (i.e., parent companies headquartered overseas) with significant U.S.-based operations?*

NTIA should ultimately consider making innovation fund awards that will boost the United States' global competitiveness in the 5G market. NTIA should not apply preferences to awardees based on the location of their operations or headquarters.

c. *What requirements, if any, should NTIA take to ensure "American-made" network components are used? What criteria (if any) should be used to consider whether a component is "American-made"?*

For the reasons discussed above, ITI strongly discourages NTIA from requiring "American-made" network components to be used in the performance of innovation fund projects. Applying BABA requirements to the development of 5G and broadband infrastructure is inconsistent with the public's interest. As NTIA previously noted when broadly waiving Buy America requirements for projects funded through the American Recovery and Reinvestment Act of 2009 (ARRA), there is a need for government-funded projects to incorporate the most modern technology in networks. Sometimes, adequate—but not the best—technology might be available domestically, but the result could mean that digital or hybrid digital infrastructure builds would not be incorporating optimal technology. It would be like telling schools that buy laptops for their students to buy ones that are slower and have less memory than those produced today. NTIA noted that waiving Buy America requirements was critical for innovation, stating that "The broadband industry is very dynamic and global, and equipment can change over the course of a buildout." NTIA noted that applying domestic sourcing requirements to grants would "ultimately slow broadband deployment and undermine the broadband initiatives."

That is just as true, if not more so today, with broadband providers considering new O-RAN technologies and other infrastructure providers considering products with rapidly evolving Internet of Things and artificial intelligence capabilities built in. This technology is developed through global supply chains and requiring domestic onshoring of these sources of supply will not boost the United States' global competitiveness.

26. How, if at all, should NTIA collaborate with like-minded governments to achieve Innovation Fund goals?

Collaboration with U.S. Government allies is critical to achieving innovation fund goals and to maintaining U.S. competitiveness abroad. Applying strict domestic content requirements to innovation fund projects will undermine these goals. In general, ITI supports increased bilateral, regional, and multilateral engagement between the United States and allied/partner economies in a manner that increases digital trade partnerships, enhances international regulatory compatibility, and reduces overall barriers to trade.

As the United States is a party to the World Trade Organization (WTO) Agreement on Government Procurement (GPA), which allows U.S. companies the right to bid on foreign government procurement contracts in the 46 other countries that are parties to the GPA, American companies benefit from a level playing field. The GPA provides U.S. companies with nondiscriminatory access to foreign government procurement markets with an estimated value of more than $4 trillion, far in excess of total annual U.S. government procurement which was valued at $488 billion in 2016 according to the Federal Procurement Data System. Thus, the GPA regime affords U.S. operations substantial opportunities in foreign government procurement markets. Separately from the GPA, the United States has trade agreements with various countries containing provisions that establish reciprocal market access in government procurement, which are also covered under the Trade Agreements Act (TAA).

Engaging the global market in satisfying innovation fund project requirements addresses compelling economic reasons for diversification of sources of supply. On a macro level, full and open competition drives down prices in markets for products and services. Increasing diversification of sources of supply also reduces the likelihood of costly disruptions. On a micro level, companies face realities that make it impossible to change supply chains overnight. They must consider a variety of factors beyond the location of their first and second tier suppliers in making sourcing decisions.

There are several different funds at this time for promoting various initiatives related to supplier diversity in the telecom space. This includes a $500 million over five years to the International Technology Security and Innovation (ITSI) Fund from the CHIPS Act. The goal of the fund is to "provide for international information and communications technology [ICT] security and semiconductor supply chain activities, including to support the development and adoption of secure and trusted telecommunications technologies, secure semiconductor supply chains, and other emerging technologies. NTIA can encourage State to work with our trusted partners in telecom supplier diversity where State can focus on supporting projects internationally that boost ICT solutions and innovative capacity in developing countries and strengthen these countries' policies to protect critical technologies. As NTIA considers awards it should coordinate with this and other funding mechanisms to prevent duplication.

Engaging international partners, including our closest allies, on supply chain issues provides an opportunity to both strengthen diplomatic ties and diversify supply chains. Engagement with allies and partners should focus on creating a trusted environment in which firms can carefully calibrate supply chains, improve global supply chain security and transparency, minimize time-to-market, and account for other considerations that enable them to remain globally competitive, while recognizing and accounting for the complexity, interconnectedness, and significant investment required to operate critical materials supply chains. ITI strongly encourages the federal government, and in particular, NTIA, to keep these global competitiveness considerations in mind and coordinate policies and strategic objectives with foreign governments to ensure the stability of the materials supply chain.

Conclusion

Thank you for the opportunity to provide comment on the Public Wireless Supply Chain Innovation Fund.