January 26, 2023

Re: NVIDIA Corp's Comments in Response to the National Telecommunications and Information Agency's Request for Comment on Implementing the Public Wireless Supply Chain Innovation Fund, Docket No. 221202-0260; RIN 0693-XC05

Dear Sir or Madam:

NVIDIA welcomes the opportunity to provide comments to the National Telecommunications and Information Agency's (NTIA's) request for comments on implementing the Public Wireless Supply Chain Innovation Fund. We appreciate the NTIA's work on this very important issue. NVIDIA believes that the Wireless Innovation Fund can greatly accelerate the adoption of Open RAN technologies, which will in turn significantly advance the nation's and world's communications systems.

The telecommunications industry is going through a dramatic change. The shift to Open RAN networks will provide diverse options, interoperability, flexibility and innovation for both those deploying telecommunications networks and their users. Based in Santa Clara, California, NVIDIA has been at the forefront of this technological revolution. We are a full-stack computing company with platforms for scientific computing, artificial intelligence (AI), data science, robotics, healthcare, networking, and telecommunications.

Innovation is at our core. NVIDIA has pioneered accelerated computing to tackle challenges that otherwise cannot be solved, including in the telecommunications space. Known as the leading expert in delivering AI on graphics processing unit (GPU)-accelerated platforms, NVIDIA is able to apply these concepts and innovations to improving and accelerating the development of Open RAN architectures. , NVIDIA believes a variety of factors will help propel Open RAN's development and deployment, including applying GPU acceleration to the software-defined Open RAN platform; improving cloud-native multi-tenancy architecture; developing digital twins for simulating and testing Open RAN at scale; and applying AI for intelligent RAN control and optimization.

Below are NVIDIA's responses to the Request for Comment:

Questions on the State of the Industry

Understanding the current state of the telecommunications industry is important to determining how any topics should be prioritized in the Innovation Fund, and what level of funding a topic should receive.

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?

The chief challenges to the adoption and deployment of open and interoperable, standards-based RAN, such as Open RAN, include:

1) *Performance needs improvement:* Commercial RAN must meet stringent performance requirements in terms of capacity, data rate, latency, coverage, energy efficiency, reliability, and security, among other areas. The technical performance of Open RAN is not yet as competitive as the traditional monolithic RAN, hindering the adoption and deployment of Open RAN at scale. Accelerated computing, cloud technology, and AI are critical to boosting the performance of Open RAN.

2) *Complexity in integration and testing:* The inherent multivendor nature of Open RAN requires extensive integration and testing to ensure the final product's performance competitiveness. Novel methods in both physical environments and virtual lab spaces should be developed to create a mature framework for integrating and testing Open RAN.

3) *Sufficient commercial incentives should be in place:* Due to less competitive technical performance and complexity in integration and testing, network operators are hesitant to deploy Open RAN at scale. This, in turn, leads to insufficient incentives for RAN vendors to develop Open RAN, hindering the technology's potential. By providing the right incentives, the Innovation Fund can help break this stagnancy and accelerate the pace of revenue realization for Open RAN.

Public and private networks have different requirements in terms of cost, efficiency, and innovation. Open RAN has the potential to be used in both these domains. The chief challenges to the adoption and deployment of Open RAN are similar in public and private networks.

As technology advances and market conditions change, telecom network infrastructure needs to be upgraded regularly to meet both current and future needs. For brownfield deployments of Open RAN, it is critical that the Open RAN equipment and functions can interoperate with legacy RAN infrastructure, ensuring backward compatibility between network functions, as well as network and handset equipment. To this end, it will be beneficial first to simulate and verify the Open RAN equipment in a virtual digital twin environment, which will reduce costs, mitigate impacts, and speed up deployments.

2. What ongoing public and private sector initiatives may be relevant to the Innovation Fund?
a. What gaps exist from an R&D, commercialization, and standards perspective?
b. How might NTIA best ensure funding is used in a way that complements existing public and private sector initiatives?

There are diverse public and private sector initiatives relevant to the Innovation Fund, covering research, development, standards, and trials of Open RAN for both public and private networks (e.g., Industry 4.0 applications). Nonetheless, several gaps exist:

- *From an R&D perspective*, there are not sufficient Open RAN computing platforms that can meet diverse needs. The Open RAN computing platforms need to be software-defined and programmable to offer the highest flexibility and foster innovation. The platforms should have native AI support, enabling intelligent radio control and automated service management and

orchestration. The platforms should also be built on open, commercial-off-the-shelf (COTS) hardware, utilize general purpose accelerator, and be cloud-based, capable of accelerating RAN workloads as well as RAN off-peak workloads such as AI, video, and edge applications.

- *From a commercialization perspective*, the pace at which the market is developing into real revenue is slow. RAN vendors are not incentivized to increase investment in development, and network operators are hesitant to deploy Open RAN at scale.

- *From a standards perspective*, there is a talent shortage and lack of consistent investment to sustain U.S. participation in international standards organizations -- such as 3GPP and O-RAN Alliance -- to develop standards for Open RAN. 3GPP is a large, open, and established ecosystem, spearheading the development of telecom standards (3/4/5G and soon 6G). O-RAN Alliance drives the mobile industry toward an ecosystem of multivendor, interoperable, Open RAN by developing standards complementing the 3GPP standards. It is critical to increase the talent pipeline and provide incentives to set standards for Open RAN.

The NTIA Innovation Fund can help close the gaps in R&D, commercialization and standards in public and private sector initiatives by focusing on the following areas:

- Support the research and development of software-defined, programmable, AI-native, cloud-based Open RAN computing platforms.
- Help increase public and private investment by accelerating the pace of revenue realization as well as increasing the value of the contribution made by companies in this space (e.g., broadening the use model of telecom networks beyond connectivity).
- Help increase the talent pipeline and provide incentives to sustain U.S. participation in 3GPP and O-RAN Alliance to develop standards for Open RAN.

3. What kind of workforce constraints impact the development and deployment of open and interoperable, standards-based RAN, such as Open RAN? How (if at all) can the Innovation Fund help alleviate some of these workforce challenges?

There are pockets of innovation that could form the basis of the next generation of Open RAN and open telecom networks. These areas lack a sufficiently trained workforce. The Innovation Fund can help fund specific courses and research both at the undergraduate and graduate levels. Such areas of innovation include:

- Wireless algorithms that leverage AI and machine learning (ML).
- Simulation and modelling of real-world wireless implementations to optimize research into algorithms and facilitate deployment.
- New programming models/languages suited to accelerated computing that will be utilized for both physical layer processing in RAN and AI/ML-based RAN intelligence controller (RIC), for example.

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?

Currently, private investment in Open RAN-related enterprises is low relative to the potential market opportunity compared to investments in areas with smaller market size. The main reasons for this are the pace at which the market is developing into real revenue, as well as the perceived valuation of companies that play just a part of the overall disaggregated ecosystem of the public telecom networks.

The Innovation Fund can help increase public and private investment by accelerating the pace of revenue realization, as well as increasing the value of the contribution made by companies in this space. This means broadening the use model of telecom networks beyond the purpose of connecting personal devices. Such models could be the use of Open RAN infrastructure within enterprise networks, as well as increased use within the public networks. Increased use could come in the form of vehicle-to-everything (V2X), smart cities, Internet of Things (IoT) connectivity, millimeter wave communication, as well as using the Open RAN infrastructure for both RAN processing and off-peak workloads such as AI applications.

5. How do global supply chains impact the open, interoperable, and standards-based RAN market, particularly in terms of procuring equipment for trials or deployments?

The last year or two have shown that global supply chain shortages of components have slowed down the pace of deployment of communication networks, including Open RAN. The range of components used in these systems is broad, but the problem worsens when there are application-specific or single-use components.

The ability to increase the use of standard COTS components is essential. Suppliers of these components should be able to build ahead knowing that the broad use opportunity of these components will minimize any potential inventory buildup in the supply chain.

Additionally, moving to more software differentiation is very important. Software-defined COTS solutions for Open RAN will significantly help alleviate supply chain bottlenecks. From a global supply chain security perspective, having such components sourced and manufactured in the United States will be beneficial. The Innovation Fund can help promote U.S.-based manufacturing entities such as the new TSMC fabs in Arizona.

Questions on Technology Development and Standards

Understanding the current state of open and interoperable, standards-based RAN and the standards that inform its development will assist NTIA in maximizing the impact of grants. Questions in this section will be used to assess the maturity of the technology and related standards to help determine which topics should receive additional investment.

6. What open and interoperable, standards-based network elements, including RAN and core network elements, would most benefit from additional research and development (R&D) supported by the Innovation Fund?

To accelerate the development and deployment of Open RAN, we believe that NTIA Innovation Fund should support research and development of the following open and interoperable, standards-based network elements:

- *Accelerated physical layer processing in distributed unit (DU)*: General-purpose processors alone cannot meet the demanding physical layer processing in a 5G RAN with large bandwidth and massive multiple-input multiple-output (MIMO) antenna arrays. It is essential to use hardware accelerators such as GPUs to process compute-heavy workloads in the physical layer. By supporting research and development in accelerated physical layer processing (channel coding, beamforming, channel estimation, etc.), the NTIA Innovation Fund will help improve the technical performance of Open RAN to be competitive with the traditional RAN, facilitating Open RAN deployment at scale.

- *Accelerated L2+ protocol stack in central unit (CU)/distributed unit (DU)*: The physical layer solution needs to be integrated with the L2+ stack using open interfaces to create a full-stack Open RAN solution. To ensure the performance competitiveness of the final Open RAN solution, it is critical to accelerate physical layer processing as well as L2+ processing, such as the scheduler. By supporting research and development in an accelerated L2+ protocol stack, the NTIA Innovation Fund will help improve the technical performance of Open RAN (e.g., higher spectral efficiency) to be competitive with traditional RAN, facilitating Open RAN deployment at scale.

- *Software-defined fronthaul*: As the transport between the baseband units and the remote radio units, fronthaul plays a key role in Open RAN. As new 5G use cases roll out, flexible fronthaul configurations have become an essential ingredient for balancing the latency, throughput, and reliability demands of advanced 5G applications. By supporting research and development in software-defined fronthaul, the NTIA Innovation Fund will help improve the support of flexible RAN topologies and reconfiguration dynamicity, which is critical for deploying Open RAN in the cloud.

- *Service management and orchestration*: The disaggregated, software-centric approach in Open RAN can help automate and orchestrate RAN workload. The Open RAN service management and orchestration layer plays a central role in key use cases such as traffic steering, quality-of-experience optimization, quality-of-service-based resource optimization, predictive service assurance, closed loop automation utilizing AI, and potentially dynamic orchestration between RAN processing and off-peak non-RAN workloads. By supporting research and development in service management and orchestration, NTIA Innovation Fund will help ensure network-wide service optimization and improve asset utilization, creating a self-sustainable and continually growing Open RAN ecosystem.

- *Advanced radio intelligent controller and applications*: Open RAN embraces AI to realize intelligent radio control and optimization. Nonetheless, the true power of AI in radio control and optimization of Open RAN is yet to be unleashed, due to a lack of access to physical layer data from commercial-grade hardware, and the difficulty of implementing AI algorithms in hardware to achieve the required inference speeds. By supporting research and development in advanced radio intelligent controller and applications, NTIA Innovation Fund will help unleash the

tremendous power of AI in Open RAN, laying a strong foundation for the long-term success of Open RAN in 6G and beyond.

7. Are the 5G and open and interoperable RAN standards environments sufficiently mature to produce stable, interoperable, cost-effective, and market-ready RAN products? If not:
a. What barriers are faced in the standards environment for open and interoperable RAN?
b. What is required, from a standards perspective, to improve stability, interoperability, cost effectiveness, and market readiness?
c. What criteria should be used to define equipment as compliant with open standards for multivendor network equipment interoperability?

3GPP and O-RAN Alliance are the two key international standards organizations that have been developing 5G and open and interoperable RAN standards. 3GPP is a large, open, and established ecosystem, spearheading the development of telecom standards (3/4/5G and soon 6G). O-RAN Alliance drives the mobile industry toward an ecosystem of multivendor, interoperable, Open RAN by developing standards complementing the 3GPP standards. Commercial 5G RAN networks have been increasingly launched globally, proving the maturity of the 5G standards developed by 3GPP. However, the vast majority of the deployed commercial 5G RAN networks are traditional monolithic RAN. The O-RAN Alliance's published specifications have set a good foundation for Open RAN development and deployment, but they require improvement for broader ecosystem adoption.

The main barriers faced in the standards environment for open and interoperable RAN include:

- *Commercial incentives*: The foundation of a vibrant standards environment for open and interoperable RAN is strong commercial interest from the ecosystem. Currently, network operators are hesitant to deploy Open RAN at scale and incentives for RAN vendors to develop Open RAN are not sufficient, impacting companies' contributions to standards development.

- *Specification maturity*: Mature specifications are the basis for Open RAN product development and successful commercial deployment. Currently, the O-RAN Alliance's published specifications have different levels of maturity. For example, the specifications on testing and integration require improvement in clarity, accuracy, and comprehensiveness for broader ecosystem adoption.

- *Talent shortage and consistent participation*: The development of open and interoperable RAN standards relies on a large group of skilled standards engineers working on the front lines of international standards organizations and many more R&D engineers working in back office to develop technology and support standards development. Currently, there is a talent shortage and lack of consistent investment to sustain contribution and participation in the standards environment for open and interoperable RAN.

From a standards perspective, the following actions can be taken to improve stability, interoperability, cost-effectiveness, and market readiness of Open RAN:

- Accelerate the pace of revenue realization for Open RAN to motivate companies to contribute more actively to standards development.

- Improve clarity, accuracy, and comprehensiveness of Open RAN specifications, such as those on testing and integration, to make the standards mature for broader ecosystem adoption.

- Increase the talent pipeline and provide incentives to sustain contribution and participation in the standards environment for open and interoperable RAN.

Standards organizations are in the right position to introduce the criteria to define equipment as compliant with open standards for multivendor network equipment interoperability. For example, O-RAN Alliance has established certification and badging processes for Open RAN-compliant equipment. It is sensible to build upon and expand the O-RAN certification initiative to facilitate multivendor, Open RAN equipment certification, adoption, and deployment.

8. What kinds of projects would help ensure 6G and future generation standards are built on a foundation of open and interoperable, standards-based RAN elements?

To ensure 6G and future generation wireless standards are built on a foundation of open and interoperable, standards-based RAN elements, we believe that NTIA Innovation Fund should support innovative, "leap-ahead" technologies that have the potential to sustain successful development and deployment of Open RAN in the long run. Key focus areas include:

- *Software-defined RAN:* A software-defined approach to implementing Open RAN reduces development time and provides flexibility compared to FPGA- and ASIC-based implementations. A software-defined approach also paves the way to 6G and future generation wireless standards that will use AI/ML to optimize telecoms networks via continuous learning and adaptation to the environment.

- *Accelerated computing with COTS hardware*: The ability to run on COTS hardware is important for the development and deployment of Open RAN at large scales in both public and private networks. It also reduces the risk of supply chain shortages. To ensure the performance of Open RAN running on COTS hardware, it is critical to accelerate the RAN computing with, e.g., GPUs, rather than solely relying on general-purpose processors like CPUs.

- *Cloud-based, muti-tenancy architecture*: Support of Cloud RAN will become central in 6G and future generation wireless standards due to its many benefits, such as flexibility and scalability. To create efficiency gains for telcos and revenue opportunities for service providers, it is important that the Cloud RAN platform can host not only RAN workloads but also RAN off-peak workloads such as edge AI applications.

- *AI-enabled radio control and optimization*: 6G and future generation wireless standards will use AI/ML at all network layers, from the physical layer all the way to network configuration and operation. We must optimize the integration of AI/ML into Open RAN development and deployment now to prepare for the development of upcoming 6G standards.

- *Digital twinning capabilities*: 6G and future generation wireless standards will incorporate digital twinning capabilities. A digital twin network is a digital replica of the full life cycle of a physical network. It can be used to help simulate, deploy, and manage Open RAN networks efficiently and intelligently. Incorporating digital twinning capabilities into Open RAN will future-proof it, making it forward compatible with 6G standards.

In addition, NTIA Innovation Fund should support participation and leadership by private sectors in international standards organizations such as 3GPP and O-RAN Alliance. 3GPP is a large, open, and established ecosystem spearheading the development of telecom standards (3/4/5G and soon 6G). O-RAN Alliance drives the mobile industry toward an ecosystem of multivendor, interoperable, Open RAN by developing specifications complementing the 3GPP standards. Sustained U.S. participation and leadership in 3GPP and O-RAN Alliance is essential to promote and drive innovative, "leap-ahead" Open RAN technologies to become the foundation of future-generation wireless standards.

Questions on Integration, Interoperability, and Certification

Challenges associated with systems integration and component interoperability can hinder the adoption of open and interoperable, standards-based RAN. This section will help NTIA structure the NOFOs in a way that most effectively addresses these challenges and facilitates adoption. NTIA also welcomes feedback on the effectiveness of certification regimes in driving open and interoperable, standards-based RAN adoption.

9. How can projects funded through the Innovation Fund most effectively support promoting and deploying compatibility of new 5G equipment with future open, interoperable, and standards-based equipment?
a. Are interoperability testing and debugging events (e.g., "plugfests") an effective mechanism to support this goal? Are there other models that work better?

The inherent multivendor nature of Open RAN requires efforts in interoperability testing and integration to ensure the performance competitiveness of the final product. Lack of mature framework for interoperability testing and integration remains the Open RAN's Achilles' heel. Novel integration and testing methods in both physical environments and virtual lab spaces should be developed.

Steering the trend of network deployments toward Open RAN requires strong industry partnerships and proactive ecosystem engagement in multivendor testing and integration efforts. Effective models that move the needle on Open RAN interoperability testing and integration include:

- *OREC (5G Open RAN Ecosystem)*: This project, launched by DOCOMO, now has 13 vendors, including NVIDIA, involved. It provides a shared open lab environment to develop, test, and integrate interoperable equipment of multiple vendors to deploy high-quality Open RAN products as defined by the industry bodies 3GPP and O-RAN Alliance.

- *OTIC (Open Testing and Integration Center)*: This initiative, launched by the O-RAN Alliance, provides a collaborative, open, and impartial working environments. OTICs are vendor-independent, open and qualified physical spaces that conduct functional, conformance, and

interoperability tests, among others. OTIC issues O-RAN-authorized certificates and badges to vendors' equipment, attesting compatibility with Open RAN standards.

In addition to physical lab space, it is also essential to have virtual lab space for interoperability testing and integration. The possibility of conducting interoperability testing and integration in a virtual environment can greatly reduce overall costs (e.g., construction cost of physical labs, expense of travel to physical labs), significantly increase test coverage, and verify Open RAN functions and performance at a large scale prior to commercial deployment.

We anticipate that digital twins will revolutionize Open RAN by allowing the simulation of the development and deployment in a virtual world prior to its realization in the real world. Open RAN deployment can be entirely simulated and configured before they are rolled out. Open, interoperable, and standards-based equipment can be tested in digital twin worlds before they are deployed. And the networks can be optimized and continuously monitored through real-time, digital twin replicas.

10. How can projects funded through the program most effectively support the "integration of multi-vendor network environments"?

Building multivendor, interoperable, Open RAN requires a comprehensive testing framework -- from the inception of the individual components to the validation of the final, integrated product. There are two flavors to this testing framework supporting the integration of multivendor network environments: component-level testing and end-to-end testing.

Benchmarking component-level tests facilitates validation of interoperability and conformance at the early stages of development. End-to-end testing provides network operators and system integrators the ability to measure an integrated system's performance and ensure fulfillment of network key performance indicators (KPIs) in a multivendor network environment before it gets aggregated to the live deployment. Developing a modular and reliable testing and integration plan tailored toward the specific needs of Open RAN is essential to accelerating the trend of greenfield, Open RAN deployments in the United States.

Projects funded through the Innovation Fund program can most effectively support the integration of multivendor network environments by promoting or enabling the following:

- Comprehensive documentation and sharing of testing recipes (including test scripts) for both component levels as well as end-to-end integrated system-level testing with the broader Open RAN ecosystem partners.
    - This would avoid duplication of effort and lower the barrier of entry for smaller vendors in the supply chain, helping to democratize the Open RAN marketplace with well-tested, quality-assured, standards-based, interoperable equipment.

- Standardization and general availability of step-by-step, well-articulated testing procedures for conformance, interoperability, and end-to-end integration testing, including test cases and expected outcomes for Open RAN vendors to use.

    - O-RAN Alliance's published specifications on testing and integration have set the first step toward that goal, but require improvement in clarity, accuracy, and comprehensiveness for broader ecosystem adoption.

- Robust, comprehensive benchmark for functionality and performance testing of various Open RAN interfaces, nodes, and elements. Traceability and reproducibility of test results should be emphasized in the established testing processes.

- Feedback loop between standards bodies alliances and the testing and integration labs, such that specifications evolve toward more mature, comprehensive, future-proof and trustworthy testing process standardization.

- Extending testing and integration initiatives beyond physical labs to field trials, facilitating deployment-readiness for the equipment tested in the lab.
    - Extending testing centers like OREC and OTIC beyond labs, with additional initiatives augmented on top of the existing facilities would be beneficial.

- Complementing testing and integration initiatives in physical labs with virtual labs, enabling cost reduction, better test coverage, and verification at scale.
    - Exploring new technologies such as digital twins to build virtual labs could be game changing.

11. How do certification programs impact commercial adoption and deployment?
a. Is certification of open, interoperable, standards-based equipment necessary for a successful marketplace?
b. What bodies or fora would be appropriate to host such a certification process?

The core principle behind successful Open RAN deployments is a solid testing and integration framework. A robust system integration infrastructure ensures that disparate RAN elements, comprising disaggregated hardware and software components from multiple vendors, can seamlessly interconnect and operate in concert to deliver superior quality service to end users.

It is critical to have an independent, collaborative, and impartial set of lab facilities to conduct testing and integration of Open RAN components and functions and certify the end results so that broader industry ecosystem can benefit from the centralized effort. Certification of standards-based equipment certainly helps in accelerating technology adoption, as is evident from citizens broadband radio service (CBRS) certification processes like spectrum allocation server (SAS) and citizens band service device (CBSD), which have been broadly adopted by the CBRS ecosystem. Enabling strong mutual authentication between servers, base stations, installers, and other systems, certificates are required for all participants in the CBRS domain. In a similar way, paving the path of Open RAN productization, operationalization, and commercialization would require the creation of a vibrant marketplace with Open RAN standards compliance equipment that are rigorously tested and certified by Open RAN standards developing bodies like O-RAN Alliance.

O-RAN Alliance, the global industry consortium standardizing Open RAN architecture, is leading the initiative of certification and badging processes for O-RAN compliant equipment. O-RAN's certification process has three tiers: a) *conformance certification*, b) *interoperability badging*, and c) *end-to-end system integration badging*. Certification and badging of Open RAN solutions developed by O-RAN Alliance ensures confidence in vendor's equipment tested and certified by O-RAN, for both the network operators and the network equipment providers community. Commercial adoption and deployment of open, interoperable, standards-based RAN can be fueled by such certification processes developed by O-RAN Alliance and hosted in O-RAN-established open testing and integration centers (OTICs) across the world.

One gap in the Open RAN certification process is the lack of adequate certificate issuing facilities in North America. Currently, there is only a single OTIC lab established in the United States (Kyrio O-RAN Test and Integration Lab). Innovation Fund can promote setting up of more such OTIC facilities across the United States to facilitate multivendor, Open RAN equipment certification and adoption and deployment. Additionally, the Innovation Fund can facilitate expansion of OREC footprint in the United States or promote collaboration between OREC and OTIC to create a centralized facility for both advanced testing platform and certificate issuance.

12. What existing gaps or barriers are presented in the current RAN and open and interoperable, standards-based RAN certification regimes?
a. Are their alternative processes to certification that may prove more agile, economical, or effective than certification?
b. What role, if any, should NTIA take in addressing gaps and barriers in open and interoperable, standards-based RAN certification regimes?

O-RAN Alliance has established certification and badging processes for Open RAN-compliant equipment. O-RAN's certification process comprises three categories: a) *conformance certification*, b) *interoperability badging*, and c) *end-to-end system integration badging*. Conformance certification verifies compliance of the devices under test (DUT) to the standards-based Open RAN interfaces using O-RAN conformance test specification. Interoperability badging assesses interoperability of pairs of DUTs following O-RAN interoperability test specifications. End-to-end system integration badging attests comprehensive system integration of a group of DUTs implemented according to O-RAN interfaces, with the testing being guided by O-RAN specifications.

O-RAN Alliance's certification and badging process is a good starting point for standards-based RAN certification regime, but it is not sufficient. Existing gaps and barriers in the open and interoperable, standards-based RAN certification regime should be addressed with the following set of resolutions to incentivize broader adoption of the certification process and democratize the Open RAN marketplace:

- Comprehensive documentation and sharing of testing recipes, including test scripts, with the broader Open RAN ecosystem.

- Standardization and general availability of step-by-step, well-articulated testing procedures for conformance, interoperability, and end-to-end integration testing, including test cases and expected outcomes for Open RAN vendors to use.
- Enhanced traceability and reproducibility traits in existing certification processes.

- Feedback loop between standards bodies and testing centers issuing certificates, including feedback from vendors undergoing equipment testing as well as experience from operators utilizing certified equipment in their deployed networks.

- Expansion of certificate-issuing facilities (e.g., OTIC labs) in North America, preferably within the United States.

- Promotion of actual field trials, including small-scale deployments in targeted environments, for verifying deployment readiness for end-to-end, Open RAN solutions.

Alternatives to certification processes, such as the OREC initiative, could be equally (if not more) agile, economical, and effective. The Innovation Fund can facilitate expansion of the OREC footprint in the United States or promote collaboration between OREC and OTIC to create one centralized facility for both advanced testing platform and certificate issuance. Innovation Fund could incentivize collaboration between North American and OREC member operators, which would be beneficial in this context.

While the entire focus of the ongoing Open RAN standardization initiative centers on the RAN component of telecommunications network, it is important to realize that RAN alone will not provide a working end-to-end system for network deployment. Seamless integration between RAN and core network and the end-to-end network optimization of both would ultimately be crucial in making the Open RAN initiative a commercial success.

Questions on Trials, Pilots, Use Cases, and Market Development

A 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 have seen a range of Open RAN trials, pilots, and use cases underway across the United States and internationally to date. This section will inform the types of NOFOs NTIA publishes and administers as the Department works to accelerate adoption.

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? What kinds of use cases, if any, should be prioritized?

We foresee diverse use cases for Open RAN in both public and private 5G and beyond networks. In our view, one of the most important use cases is to provide both connectivity services and non-connectivity services such as AI applications (e.g., drive mapping, federated learning, video analytics, predictive maintenance, factory digital twins) using the same computing platform, which we term “AI-on-5G.”

The current RAN infrastructure and the AI computing infrastructure are evaluated, deployed, and managed independently. Dedicated and overprovisioned hardware is primarily used for RAN to provide capacity for peak demand. As a result, most RAN sites on average have low utilization. This has been the industry reality for years as technology evolved from 2G to 4G. But it is set to become even more pronounced in 5G and beyond as the push for densification, combined with the use of millimeter wave, leads to a fast increase in the number of cell sites.

Using the same computing platform to enable AI workloads to run seamlessly over a 5G Open RAN network delivers both technical and cost efficiencies. It brings lower total cost of ownership for equipment, power, and space, enabling the auto-scaling and pooling of compute resources. In particular, it opens the door to dynamically orchestrating resources between RAN and AI work, providing new capabilities for smart cities, security systems, retail intelligence, and industrial to name a few.

Industrial automation is one example. AI-on-5G connects robots, smart devices, and people during all phases of industrial automation design, deployment, operations, and maintenance. Another example is a smart city application, where AI-on-5G connects cameras and provides video analytics.

In summary, we believe that it is critical to prioritize "AI-on-5G" use cases. Utilizing the same Open RAN computing platform to support both connectivity services and AI applications delivers significant improvements in asset utilization, creating efficiency gains for telcos and revenue opportunities for service providers. This will lead to a self-sustainable and continually growing Open RAN penetration from urban to rural and underserved communities and in both public and private networks.

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?
a. What kinds of testbeds, trials, and pilots, if any, should be prioritized?

Accelerating commercial deployments for Open RAN based network is a goal best achieved if related trials, use cases, feasibility studies, and proofs of concept not only aim for deployment for today's technology with Open RAN fabric, but also tailor the multivendor Open RAN infrastructure toward easy scalability and evolvability as telco embraces emerging technologies powered by AI.

Following are the few areas this program should prioritize:

- Plugfest and proof of concept events in North America (preferably within the United States) supporting the ecosystem players in testing and integration of their implementations, ensuring the openness and interoperability of Open RAN solutions from different equipment providers.

- Demo exhibitions (physical or virtual) in key industry events (e.g., Mobile World Congress), community events (e.g., workshops, tutorials), lab and field trials to promote Open RAN awareness and facilitate easy access of Open RAN tested technologies, vendors, and equipment for network operators and service providers.

- Online and in-person training and other events (such as tutorials, workshops, and online courses) to foster and develop Open RAN system integrators' technical capabilities.

- Tools and simulation platforms facilitating research and development work as well as commercial, at-scale network deployment of forward compatible Open RAN, to seamlessly extend AI capabilities in the future.

- Testbeds enabling advanced capabilities like data collection spanning the radio frequency domain through to the open, standards interfaces and digital twinning capabilities that would facilitate

easy incorporation of AI/ML control and optimization into Open RAN networks and the evolution of Open RAN infrastructure to support new and emerging use cases.

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

Existing testbeds in OREC and OTIC labs can be utilized to accelerate testing, integration, and certification of Open RAN equipment, which in turn would fuel accelerated adoption and deployment of Open RAN networks.

Another promising initiative is OpenAirInterface (OAI) 5G RAN Project, which is actively developing and delivering 5G software stack based on industry standards for Open RAN (e.g., O-RAN specifications).

Questions on Security

Strengthening supply chain resilience is a critical benefit of open and interoperable, standards-based RAN adoption. In line with the Innovation Fund's goal of "promoting and deploying security features" to enhance the integrity and availability of multi-vendor network equipment, and Department priorities outlined in the National Strategy to Secure 5G Implementation Plan, this section will inform how NTIA incorporates security into future Innovation Fund NOFOs.

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

A crucial aspect of network security in a multivendor telecommunications infrastructure is *authenticity*, which goes hand in hand with another security feature: *integrity*. Network authenticity can be breached several ways, e.g., through fake base stations or counterfeit network equipment. Enablement of robust detection and prevention mechanisms so that spurious products do not become part of an Open RAN deployment infrastructure should be deemed as one of the critical security criteria for multivendor networks. There are ways both at the software and hardware levels to address the issue of counterfeit detection and prevention, including physical uncodable function (PUF) and specialized hardware packaging (e.g., special physical coating on network equipment). Ensuring authenticity of network equipment is an integral part of a resilient supply chain.

Availability is another important security trait for the supply chain. Advanced persistent threat groups associated with nation states or state-sponsored groups generate more than 50% of the threats that can disrupt network availability and can potentially take down an entire telecommunications network, according to the report published by the European Union Agency for Cybersecurity (ENISA) on threat landscape. Cyber-crime organizations, on the other hand, can exploit network availability in a malicious way (e.g., for crypto mining), throttling network availability for authorized users. Ensuring availability of

network resources to genuine network subscribers is an essential feature for open and interoperable, standards-based RAN.

a. Supply chain is a broad landscape, involving hardware/software/firmware vendors, third-party suppliers, tool chain vendors, build environment (e.g., software code compiler), source code repository, etc. This diverse set of backdoor tool chains can be a potential attack point for telecommunications networks. Overall, supply chain security is the most crucial aspect of multivendor networks, and it is one of the weakest links that requires robust security features. Projects and initiatives awarded with NTIA Innovation Fund should ensure effective and continuous management of security issues across the supply chain by adopting security best-practices, including robust mechanisms for *vulnerability and incident reporting*. In particular, rapid patching and mitigation capabilities while vulnerabilities are detected (i.e., zero-day vulnerability mitigation) are crucial in mission-critical services like telecommunications networks, where service downtime could be prohibitively disruptive. Related guidelines from the National Institute of Standards and Technology (NIST) special publication NIST SP 800-161 on *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* can be a good reference for setting the program's criteria related to security reporting.

b. Supply chain security threats can lead to compromise of *confidentiality*, *authenticity*, *integrity*, and *availability* -- the four key pillars of secured telecommunications networks. Addressing these issues has a direct impact on the goals of the Innovation Fund. There are well established guidelines and best practices published by international standards bodies and agencies like NIST and ENISA with respect to supply chain security, including:

   - NIST Updates Cybersecurity Guidance for Supply Chain Risk Management | NIST
   - NIST SP 800-207 Zero Trust Architecture
   - Cybersecurity Supply Chain Risk
   - Management Practices for Systems and Organizations (nist.gov)
   - Understanding the increase in Supply Chain Security Attacks — ENISA (europa.eu)
   - Threat Landscape for Supply Chain Attacks — ENISA (europa.eu)

   Security frameworks and best-practices outlined in these publications can provide helpful references to understand the threat landscape, attack tactics and techniques used for compromising a supply chain, security controls and risk management, and, in turn, can shape the program's criteria for security requirements in Open RAN networks.

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

Mitigation of security concerns in Open RAN networks through deploying hardware and software advanced capabilities and security features is essential, but not enough. Building a resilient supply chain for multivendor networks also requires security-oriented discipline in the engineering processes, the hardware and software development processes, and in the entire product life cycle management (LCM). Security should be embedded *holistically* within the supply chain ecosystem, all the way from the inception of individual components to the integration of these elements into Open RAN network and their continuous LCM.

Sources of security vulnerabilities in the supply chain of Open RAN networks can be broadly categorized into *organizational*, *operational*, *technical*, and *personal* weaknesses.

- Organizational weaknesses:
  - Lack of proper employee training and cybersecurity awareness.
  - Lack of attention in the hiring process, especially inadequate background check process (e.g., while hiring third-party consultancy services). Supply chain compromises can happen due to insiders.
  - Lack of company investments in setting up robust, security-oriented processes.

- Operational weaknesses:
  - Lack of security best-practices in various stages of operations and processes, for example, software/hardware development process, testing, product LCM, vulnerability and incident management (i.e., how fast vulnerabilities can be identified, patched, and communicated safely, securely, and efficiently to the customers or end users).
  - Lack of comprehensive planning in handling security incidents. Addressing vulnerabilities without service interruption is crucial for mission-critical operations like telecommunications services.

- Technical weaknesses:
  - Lack of proper code signing, writing extremely vulnerable software, poor verification and vulnerability diagnosis, etc.
  - Lack of software quality assurance (especially security testing).
  - Lack of security features and security requirements.
  - Lack of protection in software code repository (e.g., lack of access control, lack of proper audit/logging).
  - Lack of security in IT infrastructure.

- Personal weaknesses:
  - Phishing/social engineering attacks. One useful reference is MITRE ATT&CK Framework, which explains reconnaissance techniques, i.e., how adversaries can weaponize social profiling to target employees and use phishing attacks to gain access to the company assets through compromised user accounts.
  - Various ways in which human resources can be compromised, either deliberately (e.g., for financial interest) or through deception.

These weaknesses may eventually lead to security incidences, and often stem from lack of security-minded thinking or security-oriented processes. Addressing and remedying all these weaknesses requires adequate investment by network equipment providers. Supply chain security risks touch sourcing, vendor management, supply chain continuity and quality, operational security, and many other functions across the enterprise and require a coordinated effort to address.

To that end, companies are adopting a variety of practices to manage and mitigate their supply chain security risks. These steps include, but are not limited to:

- Comprehensive security requirements management and inclusion in RFPs and contracts.
- Vulnerability and incident management, threat intelligence, threat and risk management.
- Establishing dedicated security teams to work on-site with approved vendors in the supply chain and proactively address vulnerabilities and security gaps in networks.
- Strict "*one strike and you're out*" policies with respect to vendor products that are either counterfeit or deviant from product specifications.
- Closely controlled policies for equipment purchases from approved, pre-qualified vendors.
- Secure software LCM program, including secure software distribution process (e.g., code signing, secured software repositories, malware scanning).
- Security training for all employees involved in the supply chain.
- Security handshake between software and hardware, including a secure boot process with robust authentication protocols in place.
- Automation in manufacturing and testing domains whenever possible, to reduce the risk of human error and intervention.
- Automation in detecting, investigating, and remediating cyber threats.
- Track and trace program to establish provenances for all components of supply chain and to capture "as built" component identity data to automatically link to sourcing information.
- Strict control on access provision for service vendors, including limited software access to a few authorized entities and restricted access to mechanical systems for hardware vendors with no access to control systems.

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

Strengthening the security of open and interoperable, standards-based RAN requires careful consideration of various aspects of network design and planning, deployment, and maintenance.

- *Trustworthiness of AI:* Along with the prevalent software and hardware security capabilities and features in telecommunications network, harnessing AI capabilities for supply chain security as well as the security of network lifecycle is emerging as the de-facto security trend for telecommunications networks. As the use of AI becomes ubiquitous in network fabric, it is crucial to ensure trustworthiness of AI systems. While rapid development of AI has enabled deployment of many systems based on it, more often than not existing AI systems are found biased due to a lack of data diversity and privacy protection, and vulnerability to imperceptible attacks. These

shortcomings degrade trustworthiness of AI systems. To aid AI empowerment in Open RAN networks, it is imperative to invest in R&D projects to improve trustworthiness of AI (e.g., robustness, accountability, explainability, generalizability, transparency, reproducibility, fairness, privacy preservation) across the entire lifecycle of AI-native Open RAN networks. Trustworthiness of AI should span from data acquisition to model development, to system development and deployment, to continuous monitoring and governance.

- *Openness and verifiability:* The principle of openness is at the core of interoperable, standards-based Open RAN. Open-source software (i.e., availability of source code), open specification standardizing de facto open protocols, and open, formal verification processes are the basic building blocks that would infuse "trustworthiness" into the fabric of *openness* in Open RAN networks. A trust system (RFC 4949) should operate exactly the same way it is designed for, despite environmental interferences or attempts at adversarial attacks. What makes a "trust" system "trustworthy" is the traits of *verifiability*, i.e., the trust system can be verified in a convincing way (e.g., code review and other formal verification processes). Verification is one of the critical steps toward making Open RAN truly open, resilient, and secure. If an open system is not properly verified, it is not practically deployable. Verifiability implies the ability to identify weaknesses in open specifications and protocols well in advance before being subject to threats and vulnerabilities in real deployments. Formal verification processes would ensure quality assurance for open specifications and protocols, which is crucial toward ensuring trustworthiness of Open RAN. If standards bodies, alliances, and consortiums work in silos and develop specifications without being verified and vetted by independent third-party security experts, the standardized protocols could end up being security vulnerable. One such example is the security vulnerabilities identified in 5G systems authentication protocols by independent security experts after the publication of 5G specifications. It is also crucial to have the means to fix broken protocols in an expedited way -- something that protocol testing and verification framework alone cannot do. The Innovation Fund can accelerate the maturity of openness and verifiability metrics in Open RAN by incentivizing relevant R&D projects and encouraging industry consortia in the space of Open RAN to embrace these traits in their standardization work and define a clear set of security requirements for Open RAN vendor ecosystem that spans hardware, software, system and solutions.

To summarize, taking the big leap from designing and facilitating Open RAN standards in print to accelerating its deployment in the real world requires addressing all these gaps related to trustworthiness, openness, and verification infrastructure, and channeling investments to facilitate projects that would create solutions to bridge these gaps. Innovation Fund can facilitate strengthening the security of open, interoperable, standards-based RAN by promoting and incentivizing development and deployment of Open RAN with a strong foundation based on the principles of trustworthiness of AI, openness, and formal verification.

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?

The zero-trust model applied to existing 5G network deployment is built upon three core principles:

- *Don't trust always verify* implies that getting into a network always requires authentication (i.e., end user is known, and the equipment is authentic) and attestation (i.e., computing environment is in good health).

- *Grant least privileges* means if an entity is authorized, it gets the least access privileges it needs, nothing more, nothing less."

- *Always assume breach* is based on the presumption that security breaches can happen anytime. Telecommunications networks need to protect data and workloads against such potential breaches.

Contrary to traditional perimeter-based networks (e.g., IT infrastructure), zero trust architecture (ZTA) does not trust end users and always mandates users to go through a number of steps to access network services and features. In particular, the users need to prove that the devices they are using to access the network are free of vulnerabilities, i.e., users must attest remotely that the devices are patched and running the latest version of firmware and software, etc., with the right security configurations. Identity and access management (authentication and authorization phase) is another crucial protocol in ZTA, i.e., users need to provide identifications and authenticate themselves. Typically, multi-factor authentication is utilized. Advanced identity and access management capabilities are emerging that, in addition to traditional identity and access management, also provide threat analysis and threat intelligence (e.g., check backend service to see whether the devices/user accounts are compromised in some way). Many cloud providers like Microsoft Azure, Amazon Web Services, etc., provide these advanced capabilities for identity and access management processes. 5G network is a unique network topology, with its connectivity fabric linking to many different types of nodes (e.g., network elements, IOT devices, and mobile devices). Therefore, for 5G network deployment, identity and access management becomes an intricate and important part of the network service for ensuring security of network infrastructure.

The principle of least privileges plays a crucial role in 5G network deployments based on ZTA. Restricted authorization significantly reduces the attack surface. Microsoft, AWS, and other companies are doing active research in these topics and frequently publishing recommendations on best security practices.

The foundation of ZTA is built upon the assumption that, at any point of time, there can be malicious entities present in the network. If sensitive data is being stored in the cloud or sent back and forth between network end points, encryption and integrity protection must always be on. Data must be encrypted at rest or during transit. Integrity protection with proper key management is also vital in this context. Adequate crypto and key management capabilities are needed to protect network databases against potential breaches.

The zero-trust model-based security framework will continue to evolve and play a crucial role in secured network deployment for 5G and beyond. Emerging trends in this space include the following:

- *AI capabilities*: AI for security will be prevalent, enabling automation in security. AI capabilities for information and event management functions in 5G network are growing, primarily influenced by the five pillars of cybersecurity framework: *identify*, *protect*, *detect*, *respond*, and *recover*. Especially for large network infrastructure, processing millions of notifications regarding

operating conditions of the network cannot simply be processed manually -- these have to be automated and processed by AI. It is not only about processing network data, but also about analyzing and extracting useful insights based on which networks can take meaningful actions, for which AI capability is inevitable. Automation, threat intelligence, security compliancy check, SIEM/SOAR (Security Information Event Management/Security Orchestration, Automation, and Response), etc., are various areas where AI capabilities are crucial and will be growing in the coming days. Innovation Fund should incentivize R&D projects that would proliferate generation and adoption of new AI capabilities into Open RAN networks, making the multivendor infrastructure more intelligent, efficient, automated, secure, and robust.

- *AI for security and security for AI*: AI will become an integral part of 5G security infrastructure. AI-based techniques broadly adopted in the security industry include mitigating denial of services attacks, intrusion detection systems, critical infrastructure protection, access control, malware detection and prevention of sensitive information leakage, among others. As AI is becoming pervasive in the security framework, security of AI workload itself is warranted and requires equal attention. The threat from adversarial AI is on the rise. Exploiting gaps in the security of AI workloads to subvert AI-based security infrastructure is the core agenda of adversarial AI. The methods utilized for the production of AI workloads are systematically vulnerable to new classes of security flaws, exploiting which adversaries often hack into the network and alter AI system behavior to serve malicious end goals. Investment in the R&D for AI security is crucial to make AI-based network security infrastructure for Open RAN both a reality and a commercial success.

- *Confidential computing*: The next frontier of data security, "confidential computing," augments data confidentiality *in-use* on top of traditional data security models. Confidential computing provides end-to-end data security in three phases: *protection-at-rest*, *protection-in-transit*, and *protection-in-use*. In the first phase, stored data is secured via encryption of data prior to storing or encryption of the storage device itself. In the second phase, data is securely transmitted between network nodes using end-to-end encryption or encrypted network connections. In the third phase, data under process is being protected by encryption while it is being used in the processors (CPUs or GPUs) for computation. Existing data security models adequately mitigate risks involved in the first two phases (i.e., storage and transmission of data), but fail to address the risk of data exposure while it is being processed (i.e., the third phase). Emerging data security models are poised to adopt a holistic approach of data protection that mitigates security risks across the entire data life cycle -- from transmission to storage and usage -- which is achievable through confidential computing. Such privacy-preserving computation principle and capabilities will be growing in use in telecommunications network in the coming days, as AI and big data become an integral part of the network security framework. The Innovation Fund should incentivize research, development, and adoption of confidential computing in Open RAN networks to ensure best-of-the-breed comprehensive data security in the network infrastructure.

Questions on Program Execution and Monitoring

The Innovation Fund is a historic investment in America's 5G future. As such, NTIA is committed to developing a program that results in meaningful progress toward the deployment and adoption of open

and interoperable, standards-based RAN. To accomplish this, we welcome feedback from stakeholders on how our program requirements and monitoring can be tailored to achieve the goals set out in 47 U.S.C. 906.

22. How can NTIA ensure that a diverse array of stakeholders can compete for funding through the program? Are there any types of stakeholders NTIA should ensure are represented?

To ensure broad participation in this program, NTIA should focus its efforts on expanding the software ecosystem. There are multiple tiers of stakeholders in the field. Prioritization should be given to companies that are already contributing and investing in the technology.

25. How can the fund ensure that programs promote U.S. competitiveness in the 5G market?
a. Should NTIA require that grantee projects take place in the U.S.?
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?
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"?

U.S. competitiveness in the worldwide 5G market is best achieved by U.S. companies driving wireless standards across the globe through organizations such as Open RAN. The United States' interests are best served by a robust global marketplace of companies within the United States, and in partner countries to develop and sell components and software for use at all layers of the network stack. U.S. companies should also be encouraged to participate in not only global standards bodies but also global Open RAN testing and lab initiatives such as OREC and OTIC. A portion of the fund can be allocated to ensure that US companies can participate in such bodies and consortia. This encouragement and funding also have the bonus of accelerating the work of such entities towards deploying open 5G standards.

Most U.S. 5G related companies have offices across the world and some non-U.S. headquartered companies from partner countries have significant operations within the United States. Investments should be allocated on this basis to companies having a significant presence in the United States. A similar criterion can be used when defining American-made. A sizable portion of the product, whether it be software or hardware, should be developed and manufactured in the U.S. or by U.S. headquartered companies.

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

NTIA should promote global collaboration in the acceleration of the development and deployment of O-RAN. To engage with like-minded governments, international entities like ORAN Alliance, and OREC & OTIC could assist NTIA in spurring this cooperation.

- O-RAN Alliance: Drives the mobile industry toward an ecosystem of multivendor, interoperable, Open RAN by developing standards complementing the 3GPP standards.

- OREC (5G Open RAN Ecosystem): Launched by DOCOMO, this project now has 13 vendors, including NVIDIA, involved. It provides a shared open lab environment to develop, test, and integrate interoperable equipment of multiple vendors to deploy high-quality Open RAN products as defined by the industry bodies – 3GPP and O-RAN Alliance.

- OTIC (Open Testing and Integration Center): This is an initiative launched by the O-RAN Alliance to provide a collaborative, open, and impartial working environment. OTICs are vendor-independent, open, and qualified physical spaces for the conduct of functional, conformance, and interoperability tests, among others. OTIC issues O-RAN authorized certificates and badges to vendors' equipment, attesting to compatibility with Open RAN standards.

Additional Questions

NTIA welcomes any additional input that stakeholders believe will prove useful to our implementation efforts.

28. In addition to the listening session mentioned above and forthcoming NOFOs, are there other outreach actions NTIA should take to support the goals of the Innovation Fund?

NTIA may consider the following outreach actions:

- Hosting public workshops inviting companies to present their technology offerings.

- Directly visiting and engaging technology companies.

We are grateful for the opportunity to provide input and look forward to working with NTIA as the legislation is implemented. Please contact Ned Finkle, VP of External Affairs, at nfinkle@nvidia.com if you have any questions or would like additional information.