Joint Response of:

Marist College and iPosi, Inc

Professor Casimer DeCusatis PhD
Marist College
Poughkeepsie, NY

Mr. Richard Lee, CEO
iPosi, Inc.
Denver, CO

Introduction

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 multivendor 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.

We look forward to engaging with NTIA leadership to help NTIA achieve legislative goals set forth in the CHIPS and Science Act of 2022 with specific reference to the Public Wireless Supply Chain Innovation Fund (herein the "Innovation Fund").

Responses to Docket No 221202-0260 Questions, dated Tuesday December 13, 2022 in the Federal Register, Vol.87, No. 238

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?

Global supply chains are an inevitable aspect of the open RAN market. It is highly unlikely that open, interoperable, cost-effective solutions (for test bed trials or commercial deployment) can be provided from any single nation, including the U.S. Most modern industry or academic institutions operate in dozens of nations worldwide; it is a best practice to have such organizations leverage their global standing. Further, global supply chains provide desirable features such as continuity of supply and alternate sourcing for key components, a feature which has become increasingly important in a post-COVID world. Appropriately selected partnerships help promote innovation and technology transfer and support commercial success by addressing both technical and business issues (including time to market, scalability, and cost). The global supply chain in trade also feeds technology development, literally a multi-layer stack or pipeline of physical layer up to IP and Know-How. This stack benefits both U.S. based companies and the U.S. government. Thus, preference should be given to organizations or consortiums which can demonstrate a history of innovation, including but not limited to novel technology creation (U.S. or international patents), prior research support from U.S. organizations such as the National Science Foundation, and dissemination of peer-reviewed technical results in the global technical community.

As a best practice, security for 5G open RAN technology must include threats related to global supply chains. Threats potentially arising from foreign-sourced equipment must be included in penetration testing. since it's easier to compromise an element of procured ORAN and related network equipment from component sources outside US supply chain controls, and this is a point more susceptible than to compromise the system integrators. As a baseline, the proposal should exclude from a supply chain any

organization deemed a national security risk, for example organizations listed on the Department of the Treasury's Specially Designated Nationals and Blocked Persons List. Preference should be given to proposals that include a U.S. based company and/or U.S. based academic institution as part of an interoperability test bed which conforms to Government standards including NTIA and related agencies. Preference should also be given to supply chains incorporating U.S. allied nations so as to encourage fluid software and increase depth of hardware availability.

Further, contributions from non-U.S. organizations would preferably be matched with private capital. Fund investments or grants that are matched by private capital investment should have the least restrictions (but also within appropriate security related criteria) as to the country of origin in regard to equipment, IP, licensed technology, and other deliverables, for 5G test and deployment purposes.

Please also see a related response in the response to Question 25 below.

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?

5G (as well as WIFI 6E, and in draft review, WIFI 7, expected widely deployable by 2025) relies on underlying time synchronization, location, and other PNT related services. These services increase performance, resilience and deter and overcome otherwise vulnerable security holes or attacks. This area is ripe for U.S. based technology development. 5G will also provide a platform for high precision localization in the future, making highly precise time synchronization and security mandatory across in- and outdoor environments for autonomous operations across Industry 4.0 and public environments.

New standards should address 5G network and ORAN adaptability to GPS, next generation U.S. space PNT, and U.S. made and managed infrastructures (please reference the recent SDA/DoD November RFI to implement LEO PNT to operate hand-in-glove with US MEO-based GPS). Thus, PNT-enabled 5G is an appropriate target for Innovation Fund investment to provide highest performance, lowest latency, robust 5G leadership globally.

This also ties directly to ensuring time dissemination security, as demonstrated by recently published cybersecurity zero-day vulnerabilities in standardized network timing protocols (see for example C. DeCusatis, R. Lynch, W. Kludge, J. Houston, P. Wojciak, and S. Guendert, "Impact of cyberattacks on precision time protocol", IEEE Transactions on Instrumentation and Measurement, vol. 69 no. 5 p. 2172-2181, May 2020). Time security, reliability, and resiliency are preferably based on new methods of low cost embedded indoor GPS/LEO-PNT signal capture, highest anti-jam and anti-spoof immunity, new developments in environmental sensing such as RF propagation channel measurement methods for precise government (Dept. of Defense) and commercial incumbent spectrum protection. These are just a few examples of technical areas which would directly benefit NTIA and other organizations.

15. (Includes replies related to Questions 13 and 14) How might existing testbeds be utilized to accelerate adoption and deployment?

The Innovation Fund administration should fully lever existing testbeds, in the interest of accelerating early adoption and deployment. This may include the use of existing 5G test beds and spectrum sharing developments currently underway at 16 U.S. military bases to advance the DoD's use of 5G. This also includes existing test beds supported by private industry and academia which have already

demonstrated foundational components of 5G ORAN functionality and security. Building on existing test beds helps advance 5G technology into both public and enterprise environments.

Note that this does not preclude, and indeed encourages, efficient pre-Test Bed early-stage research and development. This also provides a relatively seamless progression to enable rapid, cost-effective next stage development from U.S. research institutions where pre-Test Bed prototype evaluation, synthesis and analysis can occur most effectively.

16. What sort of outcomes would be required from proof-of-concept pilots and trials to enable widespread adoption and deployment of open and interoperable, standards-based RAN, such as Open RAN?

Proof of concept pilots and trials should incorporate an end-to-end practical environment, with multi-vendor components, vetted by one or more prospective 5G clients as solving a technical or business problem. Pilots and trials should operate for a reasonable time, and demonstrate functionality, reliability, resilience, and security for trusted timing data. This may be accomplished with a series of black box tests, to isolate individual vendor components without compromising proprietary innovative extensions in hardware and software. Interoperability with legacy systems as well as scalability for including future technologies (such as 5G powered NTN satellite infrastructure) should be included. Test results should be vetted by peer review in the technical community and disseminated as widely as possible. A well-constructed series of test plans will evaluate 5G as more than just a higher bandwidth, low latency connection, but rather as a multi-layered solution for transforming business and government systems.

17. ''Promoting and deploying security features enhancing the integrity and availability of equipment in multivendor 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?

Security reporting should be a fundamental requirement of the program criteria. Despite the evident importance of security functionality, many organizations will treat this as a cost center unless provided with a suitable incentive. The program should require design and implementation of ethical penetration testing for open RAN solutions, based on a threat matrix developed with input from the broader open RAN community. Organizations such as the IEEE P1592 committee are in the process of developing threat matrices for 5G solutions, and their work should be leveraged in designing novel pen testing requirements for open RANs.

Security-affecting data collection and reporting should become a near real time operational property of secure 5G public networks. This capability provides underlying data to security management offices within private or governmental customer networks. Currently, there is no incentive to adopt this feature since data collection isn't detailed in current industry standards and the requirements for data collection span multiple distributed organizations rather than having clearly defined ownership. Preference should be given to proposals which include detailed specifications for distributed data collection and centralized security reporting and management. For example, aggregation of data from disparate sources can be useful in tracing the propagation of cascading failures or cyberattacks and

formulating responses such as isolating key elements in a security kill chain. As another example, centralized data collection may facilitate early and precise identification of security breaches. Deviations from a security baseline are more easily identified, and it becomes easier to classify cyberattacks and affected equipment in the early stages of an incursion. Aggregated data sets may also be useful as training data for machine learning and artificial intelligence approaches to cybersecurity and system resilience.

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

Data integrity and availability are significant concerns which should be addressed to ensure the security of open, interoperable RANs. Demonstrating fundamental security features is essential to promoting widespread adoption. Further, security features must transcend the limits of conventional supply chains, single-vendor solutions, and standards organizations. Each of these groups represents one part of an end-to-end solution, and the overall solution security must be addressed. It is not sufficient, for example, to have vendors rely on standards bodies to provide end-to-end security solutions. We recommend that ongoing work in this area require a vendor agnostic security interoperability test bed. Such a test bed would incorporate a wide range of equipment, including enterprise-class mainframe servers, software-defined networking, and modern cloud computing principles. The test bed would support security testing of open RAN solutions and demonstrate that multi-vendor RAN environments do not compromise security features. In particular, best practices would include testing for zero-day vulnerabilities which impact data integrity and availability. From a cybersecurity perspective, open RAN provides a large and diverse attack surface. Results should be disseminated to the entire community, including the creation of CVE and CWE enumerations.

We expect that most vendors will offer standards-compliant solutions to common issues such as access control, data encryption, and nonrepudiation. However, many vendors will not have the resources or specialized skills to evaluate attacks based on the network timing infrastructure, especially since these attacks require an end-to-end perspective on the RAN solution. Network timing vulnerabilities can be devastating to the RAN. If a bad actor controls the timing infrastructure, for example by spoofing the most accurate time source available, causality violations may occur which impact the order of operations for authentication, key refresh, backup, and business continuity solutions, and much more. Disabling a reliable time source through a denial-of-service attack can force attached equipment into a temporal vortex, where none of the attached equipment can verify the current time of day or whether a time-stamped transaction is valid. Since these are fundamental concerns which impact all RAN equipment, a security test bed capable of evaluating these features should be an essential part of future work.

We support best practices such as reporting cyber-attacks and their identifiable characteristics, and the network or edge equipment behavior induced by the attack (such as inducing time error offsets which can be in real time identified by cross-check with other trusted time references).

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

Traditionally, security is at best a secondary concern for many companies (despite what their marketing materials would have us believe). The first concern is always functionality; getting a working product to market as quickly as possible to initiate a revenue stream. Security is viewed as a cost center, something

to be deferred until after product launch. We should expect that the minimum possible security features will be implemented by most companies in order to meet this goal. Therefore, one goal of the Innovation Fund should be promoting the design, test, and interoperability of advanced security features, particularly those features which depend on the interaction between one vendor's equipment and other components of the RAN.

Many private companies are unaware of the nature of threats or how to treat, anticipate or handle attacks on their internal systems should threats be successfully carried out. They lack a direct relationship in most cases between an attack and preventable impact to their private corporate operations and systems (other than relatively primitive data storage backup, or other basic redundancy features). Education enabled by the Fund grants could directly spur private corporate readiness to take immediate, proportionate actions against Enterprise 5G attacks.

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

Open RAN is a critical technology for 5G networks. Preference should be given to grant proposals and consortia which can demonstrate a prior working relationship with industry standards bodies, such as the IEEE and other groups.

Further, proposals should preferably include both attack surface identification/attack mitigation techniques and mechanisms to establish trusted, high quality time sources under a variety of adversarial conditions. This second point is often neglected. Cybersecurity is more than just thwarting attacks. It's important to build a framework that ensures time information is prioritized and resilient for a broad range of applications, including enterprise computing, telecommunications, financial technologies (including electronic currency transfers, credit, and securities), and other critical infrastructure. Proposals should preferably address resilience to time disruptions, providing backup or alternative means for establishing a trustworthy time source for 5G ORAN and related applications.

5G ORAN will see early commercial adoption from organizations seeking to transform their business models, rather than simply offer incrementally faster network connectivity. This includes many aspects of the so-called industry 4.0 economy, particularly financial sector and transaction management organizations, but also transportation, telecommunications, national defense, and other market verticals. For example, 5G facilitates mobile and remote workforces and remote education services, both of which use video collaboration. This in turn helps alleviate U.S. labor and talent shortages. Consequently, corporate, and educational users will increasingly self-provision their 5G ORAN solutions, with reduced dependency on wide-area mobile network service providers. 5G ORAN must therefore self-install, self-update, and in some cases self-manage across multiple vendors. Preference should be given to grant proposals and consortia which can demonstrate these principles in pre-production environments or use their pre-production environment as a client showcase for specific business solutions.

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? 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.

The ”zero trust” model needs to extend end-to-end across the open RAN, including subtended equipment for telecommunications, data centers, and other environments. This is not an easy task; zero trust requires that we validate physical and virtual connections across the RAN, including establishment of security policies, attack matrices, and authentication systems. Emerging technologies in this area should be encouraged as part of this work. For example, the network controller in a software-defined open RAN needs to be secured with its own unique policy set, since these controllers are high value targets (analogous to DNS servers in conventional networks). Further, authentication for open RAN equipment should take place as early as possible in the connection handshake cycle, ideally within the first few data packets exchanged (authentication token-based schemes need to take this into account). Since security credentials need to expire in a timely fashion and prevent authentication bypass or Bleichenbach – style attacks.

Program requirements and monitoring for 5G deployment must include bridges between conventional and more modern open RAN implementations, to appeal to the marketplace and promote widespread adoption. A test bed capable of demonstrating this transition experimentally would be very valuable.

21. Transparency and accountability are critical to programs such as the Innovation Fund. What kind of metrics and data should NTIA collect from awardees to evaluate the impact of the projects being funded?

Project metrics should include ranking security issues using industry accepted criteria such as the CVE scoring system, rather than vendor-specific systems. Within the cybersecurity community, it is best practice for security vulnerabilities to be publicly disseminated to the community as soon as possible. This transparency minimizes zero-day vulnerability windows and allows the community to rapidly develop and test security patches. Rapid disclosure using standard security forums such as the CVE and CWE system should also be encouraged. Current best practice allows for security vulnerabilities impacting a specific vendor to be withheld from public disclosure for 30-60 days while vendors develop and test a patch. After this time, full details should be made public to the community.

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?

The stakeholders should include collaboration between industry and academic institutions. Academic organizations, having no stake in the financial gain for specific products, provide a valuable test environment for open RAN equipment. Given the current difficulties in obtaining sufficient independent academic funding to support an open test bed, academic organizations should be encouraged to receive industry hardware and software on extended loan for purposes of completing their evaluations. Preference should be given to organizations which have already demonstrated the ability to identify security issues in industry-standard protocols, and who have a history of partnership with industry in networking and cloud computing.

23. How (if at all) should NTIA promote teaming and/or encourage industry consortiums to apply for grants?

NTIA should encourage teaming and industry consortiums by giving preference to applications that demonstrate a willingness to share long-term commitments to this work. This may include industry partners who provide their academic consortium partners with access to equipment on loan without requiring any initial capital outlay, or providing options to purchase such equipment in the future at a discounted rate. Academic institutions should be encouraged to work with leading industry partners in the field, rather than pursue academic projects which may have a much longer horizon to market.

This should also include adoption of work products into O-RAN standards performed under Innovation Fund grants.

24. How can NTIA maximize matching contributions by entities seeking grants from the Innovation Fund without adversely discouraging participation? Matching requirements can include monetary contributions and/or third-party in-kind contributions (as defined in 2 CFR 200.1).

NTIA should allocate perhaps half the Fund toward programs that must match grant money with private contributions to some degree. This includes both monetary matching and in-kind contributions (i.e. use of expensive, specialized enterprise grade or telecom grade hardware and software in a realistic test bed). Matching funds or in-kind contributions demonstrate commitment from consortium partners and imply strong market demand with reduced market adoption risk. Matching funds should preferably be used to facilitate multi-vendor testing of solutions which have demonstrated technical feasibility and are poised to enter larger scale commercial deployment.

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''?

From a security perspective, existing government restrictions on foreign technology should be leveraged by this program. For example, organizations listed on the U.S. Dept. of the Treasury Specially Designated Nationals and Blocked Persons List should be prohibited from participating.

Since any viable consortium will include academic institutions, it is to be expected that students who are non-U.S. citizens may be included in funding opportunities for this work. This should be allowed, since the security risks are minimal and manageable; further, this provides a way for consortiums to leverage emerging world-class student talent and build pipelines for hiring students trained in this field in the future.

Commercial objectives suggest that an over-emphasis on American-made will retard or deter matching investments that provide substantial financial and technological "multiplier effects". Such effects are important to U.S. based 5G innovation, since they have been demonstrated to reduce time to market, improve technical resilience, and increase scalability to a global level.

Without compromising the nation's network security at every level, we recommend matching grants that aim to increase commercial adoption should not be limited to U.S. only manufacturing. Much of this innovation will result in productive trade by intellectual property and know-how, not strictly

confined to physical manufacture. This approach to shared collaboration should be seen as productive and positive, especially within and between North America, Japan, South Korea, New Zealand, Australia, the United Kingdom, and other important NATO member nation governments and markets.