SECURE G

Before the

**DEPARTMENT OF COMMERCE**

**National Telecommunications and Information Administration**

Washington, DC 20230

In the Matter of )
) Docket No. 221202–0260
) RIN 0693-XC053
Public Wireless Supply Chain )
Innovation Fund Implementation )

## COMMENTS OF SecureG

### Introduction

SecureG appreciates the opportunity to respond to the National Telecommunications and Information Administration Request for Comment. The Public Wireless Supply Chain Innovation Fund (the Fund) is a momentous opportunity to ensure Open RAN functionality and scalability come to fruition in the United States and globally.

At SecureG, we build security solutions for the next generation of networks and critical infrastructure. Created by security and network experts with decades of experience in public key infrastructure (PKI), telecom, networking and cybersecurity, SecureG saw the need to protect emerging use cases for IoT, 5G, industry 4.0, supply chains, and digital transactions.

Protecting critical infrastructure is one of the most significant challenges facing the U.S. today. Rather than extending the patchwork of existing security measures, SecureG is creating a standards-based solution built on a foundation of PKI to meet the needs demanding use cases.

Today's world is defined by connectivity. The Internet bridges local and global organizations and markets, bringing together people, machines, and data.

SecureG is pleased to respond to questions on the implementation of the Fund to expand understanding of the cyber security problem space and potential approaches and solutions. This RFC addresses many of the questions that are important to consider, specifically, practical challenges around the role of standards, zero trust, and 5G.

In our comments, we will highlight the following:

- Standards are necessary but alone do not provide a guarantee of interoperability or security. Other work needs to be done in areas like specifications that provide the details for interoperability and a zero-trust approach to security.
- Funding should enable and encourage "non-traditional" companies principally serving the private sector to participate in public sector contracts without the burden of the FAR or DFAR that would otherwise be prohibitive financially to the smaller innovative companies.
- In order to maintain U.S. technology leadership, government funding should also be made available for "seeding" the future market to provide financial incentives small companies and innovators to drive private investment.
- The security for open and interoperable, standards-based RAN will require the application of a rigorous zero-trust approach to achieve "enhancing the integrity and availability of equipment in multi-vendor networks."
- The Innovation Fund must have security-focused solicitations, or the security emphasis will get lost.
- Continued work must be done on the zero-trust model across the 5G space and should be a priority for all providers of the supply chain for 5G deployments made in critical mission areas (e.g., critical infrastructures.) The importance of zero-trust architecture is especially relevant as 5G has the potential to be the most secure if there is common acceptance and implementation of standards in this area.

**Public Wireless Supply Chain Innovation Fund Implementation**

**Section I: State of the Industry**

**Question:** 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?

Standards are often incomplete or purposely written to allow for differences in implementations. Often the differences are the kind involved in competition, vendors adding features for market advantage that does not impact interoperability. These differences show up in implementation like those represented in specification 33.501 of the 3GPP R15 (5G). Specification 33.501 provides three choices: 1) mTLS, 2) IPSec or 3) perimeter for securing the virtual network functions (VNFs) in a 5G Core or RAN. Two different 5G deployments can be fully interoperable but make different security decisions, one implementing mTLS for mutual authentication, the other relying on their network perimeter-based security, no use of mTLS or TLS protocols. The mTLS-implemented solution is consistent with the concept of zero trust that is being mandated within the Federal Government. The other is not and would continue a reliance on perimeter-based security that we know from hard experience is an insufficient means of protection. The private sector implementations have no mandate for zero-trust architecture (ZTA), and no requirement yet seen that these private sector integrators are required to apply mTLS as a method of meeting the ZTA principles in their federal client deployments. Consider what this means. The standards are not sufficient by themselves to assure that a ZTA-informed approach to security has been designed in the OTA funded 5G contracts. Requirements for best practice approaches like the use of mTLS in the 5G virtual network functions will need to come from the government to assure that ZTA does not remain just something in concept. The standard leaves it as a choice to applying mutual authentication or keeping a reliance on perimeter-based security. It is best to be clear about what that choice should be for mission critical communications.

**Question: What ongoing public and private sector initiatives may be relevant to the Innovation Fund?**

The DoD 5G initiative has seeded the financial incentive for the public sector marketplace. It is a public and private sector initiative that has allowed “non-traditional” companies principally serving the private sector to participate in the public sector OTA contracts. This is an important innovation in government contracts. These “non-traditional” companies now have a means to participate without the burden of the FAR or DFAR that would otherwise be prohibitive financially to the smaller innovative companies.

**Question: What gaps exist from an R&D, commercialization, and standards perspective?**

Standards are written by parties that are profit-driven commercial entities that want to achieve the common goal of interoperability and at the same time to advance competing interests for their position in the marketplace including international economic advantages. These are competing agendas. Standards alone are not enough to achieve commercialization. They need specifications / RFCs and agreed-to best practices to achieve interoperability at scale.

Commercialization sometimes requires “seeding” the future market to provide financial incentives to drive the private investment.  The 3GPP Phase 1 deployments have the financial incentive from a growing consumer market for bandwidth intensive applications like streaming video. The financial incentive is already built in. The 3GPP Phase 2 deployment of use cases where ultra-reliable, ultra-low latency and security interoperability do not yet have the same consumer base. These Phase 2 capabilities remain in the future, early projections for deployments already delayed by years. Unlike Phase 1 that has an existing consumer market, Phase 2 will require financial incentives (from government) to achieve commercialization, to, in effect, create that early-stage market within the federal government that can expand into a commercial scale capability. Phase 2 needs the government to provide the seed funding. Beyond the financial gap to seed the investment is also the gap of specifications / RFCs and best practice adoption. The two gaps are intertwined, without the seed funding the work to develop these specifications / RFCs will languish and delay adoption leaving the opportunity to others making that investment getting to market with solutions from other parts of the world.

**Question: How might NTIA best ensure funding is used in a way that complements existing public and private sector initiatives?**

DoD's 5G OTA contracts have provided the seed financial incentives for applying the capabilities at a technical level to achieve capabilities at an operational level – the use cases. The market incentive is seeded with this kind of R&D funding giving it a better chance to achieve at scale and persistent market adoption. Widespread adoption remains a future to be realized. The same needs to happen for ORAN or the world will simply buy proprietary solutions and there will be no Open RAN.

## Section: Trials, Pilots, Use Cases, and Market Development

**Question: How might existing testbeds be utilized to accelerate adoption and deployment?**

There is an existing testbed called the 5G Security Test Bed (5G STB)[1] hosted by CTIA – The Wireless Association, The MITRE Corp, the University of Maryland and members that includes SecureG. This testbed is directly working on many of the issues identified here and following a specific process intended to create real-world operational conditions using commercial equipment.  NTIA should consult with successful test bed deployments, like 5G STB, to better understand how we can build upon, and not duplicate work. Additional funding leveraging the work already done here to put together the cohort of companies and stakeholders can help accelerate the schedule and put the imprimatur of the government's interests / requirements in this work consistent with the idea of private-public partnerships to achieve common goals.

[1] 5G Security Test Bed Information Sheet, available at https://5gsecuritytestbed.com/wp-content/uploads/2022/06/STB-One-Pager_061422.pdf, (last accessed Jan. 24, 2023).

**Section: Security**

**Question: 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?**

The security for open and interoperable, standards-based RAN will need to apply a rigorous ZTA approach to achieve "enhancing the integrity and availability of equipment in multi-vendor networks." Telecom is one of the Department of Homeland Security's sixteen defined critical infrastructures. It is arguably the most important as it takes mobile communications to coordinate emergency responses, natural or man-made, to recover other impacted critical infrastructures. For this reason, the nation's mobile telecom would be a first target for an adversary – to deny national leadership and first responders the ability to coordinate a response and to deny command and control and computer communications. Consider the following points:

> **The Supply Chain:** An adversary's long-term cyber strategy starts with becoming an integral part of the targeted supply chain and using that dependency to integrate a means of entry into the network with the compromised components. Supply chain integrity is one of the principal concerns that motivated the CHIPS and Science Act of 2022. In telecom, the market of OEM vendors may have their proprietary products, but their system components come from its partners – including those who would be our most capable adversaries in a conflict. The same applies to Open solutions like ORAN that will also be comprised of many component providers. It is how advanced militaries operate.
>
> **Availability Means Resilience:** Protecting information system availability is principally thought in the context of uptime to meet a service level agreement. The concern for availability described here is better defined as resilience. Resilience in this context means a communications system able to a) deny an adversary's progression through a cyber kill chain and the ability to b) persist in its full or a controlled-degraded operational state even under the most adverse conditions. Where Open RAN will play a part in next generation mobile communications, resilience is assurance to communicate during a crisis. System resilience means survival so that the nation can still communicate and recover the targeted critical infrastructures.
>
> ZTA is critical by setting the high bar needed to achieve resilience. The question that remains is how to get there starting from a set of ZTA principles defined in a NIST Special Publication to an implementation and ultimately deployment suited to the criticality of mobile telecom including the implementations of Open RAN.
>
> **Solving for Provenance:** Provenance (sourcing and lineage) in the supply chain is another important component. What is on the cover of the technology device only reveals a brand but not the component resources (e.g., the micro-chips, firmware, etc.). The brand does not reveal whether the component parts are from trusted sources or whether they are from sources that could pose a threat to achieving resilience. The

provenance requirement becomes critically important. Provenance applies not just to the factory but also downstream in the technology supply chain, at the points of technology integration and operation. An example is to use provenance attributes in the X.509 certificate protocol for the execution of policy decision and policy enforcement as prescribed in the ZTA core logical components. This has potential applicability for avoiding certain networking equipment considered unacceptable in a high trust network path.

**Recommendation:** For this reason, we recommend that security should have its own solicitation, not be an add-on part of a functional use case. This has been and continues to be the problem of what happened with the DoD 5G OTAs. There is no current solicitation for security that was truly about security. There was no security architecture requirement, no security interoperability requirement that addressed how to operate across many trust domains even crossing public and private sector networks. Any system-level implementation will have many domains of trust. With no basis for determining whether these trust domains are indeed trustworthy, whatever security solution gets implemented may be entirely compromised even at the deployment. The lessons of the SolarWinds incident are instructive, where SolarWinds was touted as a network management application and a security application, so it was trusted without the proper controls to determine if it really was trustable at installation / provisioning and in operation.

**Question: What role should security reporting play in the program's criteria?**

It should play a central role. The cybersecurity framework (CSF) from NIST provides the model for understanding the role, that security is comprised of several capabilities – to identify, protect, detect, respond and recover. All these component parts of the CSF require reporting – why a security operations center is a part of every deployed instance of enterprise security protections. By example, NIST SP 800-207[2] describes the logical components of a ZTA including the Policy Engine that is the recipient of data from the Security Information and Event Manager (SIEM) where the security reporting is processed.

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

Standards, best practices, and frameworks are essential to provide a common basis for making security decisions at design, implementation, operation, and maintenance. Their role is first to provide a common basis for the developing an architecture, the language of security, the security controls that get applied and to guide the design / development / integration / implementation / operation. Consider adding the ZTA principles to this list.

**Question: What steps are companies already taking to address security concerns?**

SecureG is engaging in the role that Public Key Infrastructures (PKI) and specifically next generation PKI will play. The role of PKI as applied to the control plane elements and virtualized

[2] NIST, Zero Trust Architecture, Special Publication 800-207 available at https://csrc.nist.gov/publications/detail/sp/800-207/final (Aug. 2020).

infrastructures is our area of focus. It begins with attestation, the ability to embed an identity on system resources.  Microchips is one example that can be used to establish the sourcing provenance. Knowing the source of the chips suppliers and using that knowledge for attestation is a starting point, the IEEE 802.1AR for manufacturers of initial devices (IDevID) identity and using that as the starting point for creating a chain of trust, approved chips from an approved chip manufacturer leveraged before assigning the Local Device ID (LdevID) to continue the chain of trust at the point of integration, where the OEMs aggregate all the component parts, software to create the network elements. The third point of the supply chain is the point of delivery, the applications and services that are often hosted in data centers / the cloud that apply further virtualization (virtual machines and containers). PKI plays a central role here, the kind built for the scale and speed of the 5G Radio and Core. SecureG is a provider of the PKI, the NextGen PKI made for the critical infrastructures described as connected devices, of machine sensors, IoT, Industrial IoT and Industry 4.0

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

Restating thoughts expressed earlier that the Innovation Fund needs to have security-focused solicitations, or the security emphasis will get lost. Here are examples of the security elements for the solicitation that would be needed:

- A high-trust next generation PKI that can pass government Authority To Operate (ATO) requirements based on NIST 800-53 R5, Risk High Operations built for agencies and their critical mission areas.
- Development of a security architecture for 5G to achieve ZTA,
- Security interoperability across many trust domains including crossing public and private sectors,
- Security for virtualization, virtual machines, and containers
- Security at a system level (end-2-end) for consistent interoperability and means of determining / validating trust domains,
- A means of implementing Provenance to determine source for critical supply chain components

**Question: 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?**

This is a most critical question. It should be asked across providers, OEMs, Carriers, Integrators, Chip Manufacturers. All providers of the supply chain for 5G deployments made in critical mission areas (e.g., critical infrastructures) should be asked this question. The importance of ZTA is vital for this mobile, next generation 5G communications that have the potential to be the most secure but only if there is common acceptance and implementation of the points made earlier about the three options in specification 33.501. ZTA is not in the standards for 3GPP Release 15 or 16 and is not by itself a standard. The path between ZTA principles and a ZTA implementation/deployment is determined by the suppliers, integrators, and service providers. There is much work that needs to be done where the fund can be effective in seeding that work.

We highlight again the example of the 5G Secure Test Bed (5G STB) work being done by CTIA, the MITRE Corp, the University of Maryland, and members of the testbed that includes SecureG.

In conclusion, the decisions and investments taken now to solve for the challenges identified in the questions and answers will in no small measure determine the outcome for a safer future digital marketplace. By extension this also means the security of the country. The funds are needed in the right measure and to the right tasks. We believe that the insights we offer will help show that we have been in the advance team working these issues and developing the capabilities that can be brought to the market. Again, we appreciate the opportunity to express our thoughts on the Fund and look forward to participating.

/s/ Mike Denning
CEO, SecureG