January 27, 2023

Hon. Alan Davidson
Assistant Secretary for Communications and Information and NTIA Administrator
National Telecommunications and Information Administration
Department of Commerce

RE: Comments in response to NTIA Notice and Request for Comment on "Public Wireless Supply Chain Innovation Fund Implementation"

Palo Alto Networks appreciates the opportunity to provide comments in response to the National Telecommunications and Information Administration's (NTIA) Notice and Request for Comment (Notice), "Public Wireless Supply Chain Innovation Fund ("Innovation Fund") Implementation." Our submission addresses questions posed in the security section of the Notice to help inform how NTIA should incorporate security into future Innovation Fund Notices of Funding Opportunity.

Palo Alto Networks is the global cybersecurity leader, securing the networks and information of more than 60,000 enterprise and government customers in 150+ countries to protect billions of people globally. 95% of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cybersecurity posture. Our customers include organizations across all verticals, including telecommunications service providers and other mobile network operators (MNOs) globally. Many of these operators are deploying—or planning to deploy—5G networks. We also serve an array of enterprises, such as in manufacturing and utilities, as well as government agencies, that are deploying or considering using private 5G networks, often leased from telecom providers.

Palo Alto Networks is a recognized technical leader in 5G (and 4G) security. We are engaged in and contribute to several industry organizations that represent mobile network operators (MNOs) and the mobile ecosystem, including groups that issue standards and technical reference documents that are used by operators worldwide. In November 2020, we launched the industry's first 5G-native security offering. Palo Alto Networks was honored to provide our expertise in development of the FCC's Communications Security, Reliability, and Interoperability Council VIII report on the role of virtualization technologies in promoting 5G security. Palo Alto Networks is a collaborating vendor in the National Institute of Standards and Technology (NIST), National Cybersecurity Center of Excellence (NCCoE), 5G Cybersecurity project and made key contributions to the draft NIST Special Publication 1800-33B on 5G Cybersecurity. Our 5G security solutions are also featured in the NIST NCCoE 5G lab. Palo Alto Networks also contributed to the Open RAN Policy Coalition's April 29, 2021, paper titled *Open RAN Security in 5G*.

Palo Alto Networks' Feedback

When implementing the Innovation Fund, NTIA must revisit the conventional approach to the security of telecom networks and promote or incentivize enterprise-grade security. This process can play a critical role in promoting the prioritization of cybersecurity considerations and investments in 5G network planning and deployments—whether they are Open RAN or traditional RAN—in the United States as well as abroad. The promise of open and interoperable, standards-based RAN can be most fully realized through enterprise-grade security, which means the ability to secure the service, technology, and application stack by securing all layers (signaling, data, applications, and management), all locations, all attack vectors, and all software life cycle stages. It is foundational to enabling organizations to take a Zero Trust approach to their multi-vendor networks, including applying security on the network slice level. The projects and initiatives funded through the Innovation Fund should recognize these principles as foundational security elements to build upon.

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?

5G adoption is growing rapidly across numerous industry verticals worldwide—bringing a new threat landscape that complicates both the management of the security of telecom networks and the data that runs on them. It is not unusual for some stakeholders to consider only the security or trustworthiness of particular technologies or vendors in the network, but narrowly focusing on vendor supply chain security does not account for how telecom networks are architected or operated. It also does not capture the full picture of cybersecurity threats and risks to networks and end-users, leading to ineffective management of all risks.

Security technologies used in the past (and in many current networks) are incapable of securing the 5G opportunity of the future. Security for 3G and 4G was not focused on detecting and preventing attacks on all layers, all locations and interfaces, all attack vectors, and all software life cycle stages. While physical elements, such as hardware switches and routers still exist, today's telecom networks are dynamic and scalable, largely software-driven, virtualized, decentralized, and cloud-ready. Networks "mix and match" multiple vendors from across the globe, producing various technologies that must be integrated seamlessly. The massive increase in network connectivity, move to software-driven networks, and emergence of new types of applications pose expanded security risks for both telecom operators and their end-users/customers. Network infrastructure, applications, and services face considerably more sophisticated cyberattacks and threats, which are amplified in 5G where attacks leverage greater speeds and new points of attack as IoT devices proliferate.

The Innovation Fund program must revisit the conventional approach to the security of telecom networks and promote or incentivize enterprise-grade security. Telecom operators must secure the network infrastructure and communications/data traversing networks, regardless of the underlying technology or vendor in the network. The program should prioritize the following criteria when evaluating the role of security within its projects and initiatives:

- ***Maintaining constant real-time visibility and enforcement.*** Telecom operators need to have constant real-time visibility and enforcement of traffic interactions between and among diverse network elements as well as into and out of the network itself and be able to detect and stop in real time cybersecurity threats within that traffic.
- ***Leveraging real-time mitigation.*** This is critical in responding to correlated threats and to taking actions.
- ***Authenticating that devices and users are who they claim to be*** before they can perform a certain action, such as requesting data.
- ***Controlling the level of access each device or user is granted*** *to certain resources, based on sensitivity or criticality.*
- ***Internally dividing/segregating network elements,*** based on level of risk or function, and managing communications between disparate elements accordingly.
- ***Securing the "containers" used to build the 5G core.*** As container adoption rises, so should the adoption of best practices for container security.

These capabilities can incentivize vendor best practices while securing modern telecom networks, communications, and data regardless of the underlying technology or ICT vendor in the network.

It is also important that the Innovation Fund recognize some of the security benefits of Open RAN, as outlined in the *Open RAN Security in 5G* paper published by the Open RAN Policy Coalition, to which Palo Alto Networks contributed. These include allowing operators to, 1) build upon the capabilities enabled by 5G to shift the security capabilities closer to the edge of the network and stop attacks closer to the source, 2) integrate best-in-class security platforms with open interfaces defined to be secured using modern, industry-standard security protocols, and 3) speed the complete automation of network management. Open RAN supported by cloud-based services will also increase the speed with which operators can install software and operating system security patches, thus enabling the operator to minimize the amount of time a vulnerability is in the network.

17A. What role should security reporting play in the program's criteria?

The Innovation Fund should promote adherence to best practices and underscore the importance of promoting the integrity and availability of multi-vendor networks with a narrow focus on enterprise-grade security being built into all network layers rather than creating new

security reporting regimes that should ideally be coordinated and deconflicted with the deliberative rulemaking process currently underway pursuant to the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).

At Palo Alto Networks, we implement a number of best practices for our own transparency and software supply chain assurance. In particular, we employ a secure “shift left” approach that focuses on integrating security tools into the engineering lifecycle early on to help detect any inadvertent vulnerabilities in our code—making security synonymous with development. NTIA should embrace a holistic approach to network security and encourage the adoption of Zero Trust architectures.

17B. What role should security elements or requirements, such as industry standards, best practices, and frameworks, play in the program's criteria?

Palo Alto Networks encourages adherence to consensus-based international cybersecurity standards, reference designs, best practices, and mobile security patents to be included as a foundational requirement to receive grant funding.

As the 5G digital environment opens the door for diverse players beyond traditional cellular networks, establishing the right security approach across networks is critical. Standards development, industry organizations, and government can play a key role in identifying and promoting standards and best practices to operators and associated vendors around the globe. There have been an array of standards and best practices released on other aspects of 5G—such as spectrum allocation and use—but not as many on the leading-edge security practices.

Frameworks such as MITRE FiGHT (5G Hierarchy of Threats) are critical to establish a common definition and database of vulnerabilities, threats, and Tactics, Techniques, and Procedures (TTPs) related to 5G networks. The MITRE ATT&CK framework has done this incredibly well for general IT networks, and the same needs to be supported in mobile networks now that these networks are beginning to open up.

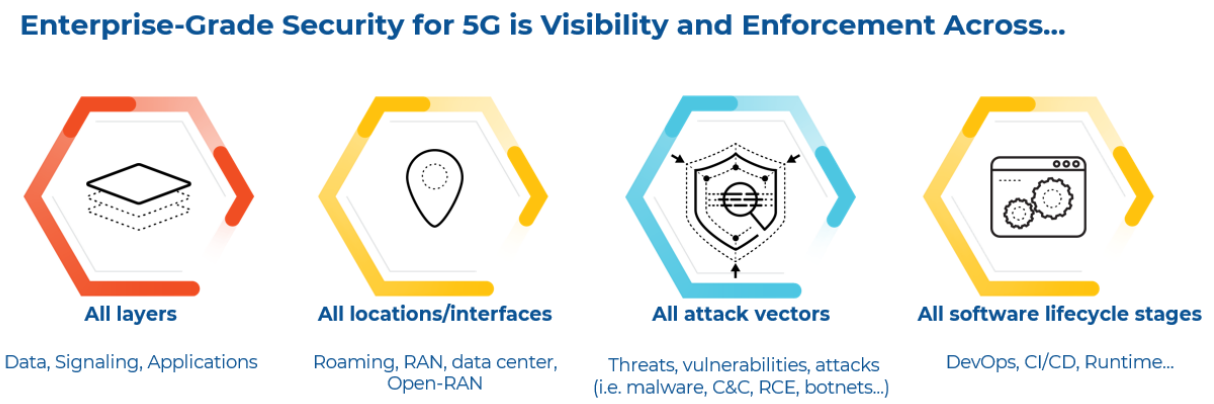
18. What steps are companies already taking to address security concerns?

The risk of cyberattacks to all organizations will exponentially grow with the scale enabled by 5G, which will dramatically increase network capacity and attack surface, particularly as an unprecedented number of devices attach to enterprise and government networks. When IoT devices are attached to 5G networks, cyberattacks can have an impact on those devices’ performance, usability, and services (i.e. reduced device battery life), in addition to causing potential network congestion or outages.

You cannot secure what you cannot see, and businesses must establish a strong security posture that can stop cyber attackers from infiltrating their networks, disrupting critical services, or destroying industrial assets. Palo Alto Networks prioritizes the detection and prevention of attacks on all layers, all locations/interfaces, all attack vectors, and all software life cycle stages.

To help manage increasingly complex and dynamic environments, Palo Alto Networks leverages artificial intelligence/machine learning (AI/ML)-driven automation, a necessity to demonstrate confidence that 5G provides enterprise-grade security. Automation and ML should be at the core of 5G security to analyze vast amounts of telemetry, proactively assist in intelligently stopping attacks and threats, and recommend security policies. ML models should be used in both out-of-band detection and in-line to help prevent previously unknown attacks and threats.

When setting out to secure telecom networks, Palo Alto Networks pursues the following steps in our enterprise-grade security strategy:



All Layers. The first goal when starting out to secure 5G is to have visibility and constant real-time monitoring across 5G signaling and 5G data layers to be able to spot any security threats and attacks. The next step is then adding the ability to automatically prevent known attacks, threats, and vulnerabilities that were detected by constant real-time monitoring. Security automation is critical in correlating threats to the attack source and to isolate those infected subscribers and devices before botnet attacks can potentially take place, offering actionable insights for faster security troubleshooting. Application-layer security has a few dimensions. Applications must be identified and confirmed if they are what they claim to be, and either allowed or blocked (or certain applications should only be allowed to be used altogether). Badly written applications can cause damage, such as by using excessive CPU, memory, or other resources, or even cause network congestion and outages.

All Locations/Interfaces. Our enterprise-grade security is able to secure all locations and interfaces. When malware takes control of IoT or mobile devices, it can coordinate simultaneous data layer attacks from thousands of infected devices via a command-and-control server. Such an attack will not come from the usual suspect of an internet-facing interface but via an interface from infected devices. Without adequate security on the latter, the 5G core network may suffer from resource exhaustion and perhaps even outages. Additionally, the roaming interface from another network (or another country) should never be trusted and always secured.

All Attack Vectors. The ability to detect malware, ransomware, command-and-control traffic, remote code execution, remote information retrieval, authentication bypass vulnerability, remote command injection, and brute force attacks is critical for enterprise-grade security. Palo Alto Networks' Unit 42 threat research team found that 41% of attacks exploit device vulnerabilities as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses. The monetary risk of not protecting against all attack vectors can be huge.

All Software Life Cycle Stages: All stages of the software life cycle across the build, deploy, and run stages of today's continuous integration, continuous development (CI/CD) approach must be secured. The core 5G network is fully containerized and is built for Kubernetes environments, and cloud security posture management, cloud workload protection, cloud network security, and cloud infrastructure entitlement management are critical.

An additional aspect of enterprise-grade security for 5G is network slice security, a fundamental 5G differentiation compared to all previous generations of mobile networks. A network slice is effectively a complete end-to-end network. 5G allows service providers the ability to offer different dedicated end-to-end network slices with different bandwidth and quality of service (QoS) to different enterprises, vertical industries, and government agencies on the same 5G network simultaneously. New slices can be launched and modified dynamically using 5G Network Slice-IDs (NSSAI) running on the 5G signaling layer. In addition to bandwidth and QoS, each slice's security level can be tailored to its specific requirements. Different network slices can also run side by side for different purposes and have their own security requirements applied to meet their respective needs. As real-time threat detection and prevention is paramount, this should be done dynamically so that traffic can be correlated to specific slices and security can be applied in real time. The ability to apply different security policies per 5G slice will help to give enterprises and governments the confidence to use 5G for their core business activities.

For reference, DISH Network Corporation has selected Palo Alto Networks to assist with securing the United States' first cloud-native, Open RAN-based 5G wireless network. DISH will

leverage Palo Alto Networks for container security, secure network slicing, real-time threat correlation, and dynamic security enforcement. DISH will use Palo Alto Networks' industry-first, cloud-native security offering, including the VM-series and CN-series Next-Generation Firewalls, as well as Prisma Cloud — the only comprehensive, cloud-native security platform on the market today.

Additionally, Palo Alto Networks has been selected by communications technology company TELUS to secure its 5G network and provide real-time threat mitigation. TELUS will leverage Palo Alto Networks' hardware and software firewalls to protect high-capacity network interfaces across its 5G stand-alone core and internet perimeter as well as to provide security to its IoT customers. Palo Alto Networks will leverage its Zero Trust approach, a security framework that is rigorously applied through the full ecosystem of controls — network, endpoint, cloud, application, IoT, identity, and more — and that many organizations rely on for protection that goes beyond the traditional network edge.

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

Since many of the use cases for open and interoperable, standards-based RAN are conceptual, the Innovation Fund should serve as a catalyst to ensure the necessary research, development, and maturation of the enterprise-grade security model. The Innovation Fund can also incentivize potential recipients to demonstrate they are meeting foundational cybersecurity criteria, including those outlined above, by instituting security-specific conditions. The program can create challenges and/or competitions, potentially as an extension of the NTIA's 5G Challenge, meant to demonstrate Zero Trust-based security for open and interoperable, standards-based RAN.

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?

Extending Zero Trust security into 5G with machine learning-powered next-generation physical and virtual firewalls helps protect end-to-end 5G infrastructures across all layers and key locations of the distributed, cloud native, multi-cloud 5G architecture. Segmenting 5G networks for Zero Trust access, an architectural security strategy rooted in the principle of "never trust, always verify," can also reduce the volume and impact of cyberattacks. It can ensure that network elements act only according to their defined role and do not have unauthorized interaction or communication with other parts of the network or outside the network (e.g., trying to connect to an unauthorized external C2 server in order to pass sensitive data). Further, if one part of a network is impacted by a threat, the threat cannot move to another part.

In the Open RAN context, it is essential to apply Zero Trust to secure the technology and application stack. It is necessary to secure all layers (signaling, applications, management, and data layers), interfaces and APIs, and all attack surfaces in an automated manner. For example, both inbound and outbound malicious activities on the data layer can be detected and controlled, such as malware, botnets, exploits of network services, and command-and-control. Operators can secure APIs in numerous ways, including by choosing security actions to be applied to requests which do not comply with an API's expected behavior, and by implementing simple baseline API hygiene activities.[1] Finally, technologies exist and continue to be innovated to reduce and secure attack surfaces across all infrastructures, including Open RAN. Operators that deploy Open RAN are able to detect and control new security attacks and threats vectors that allow suppliers, test equipment manufacturers, wireless carriers, and network operators to assess and manage security risks.

Conclusion

NTIA's implementation of the Innovation Fund—and the U.S. Government more broadly—can play a key role, including internationally, in promoting open and interoperable, standards-based RAN by incentivizing enterprise-grade security leveraging automation and ML and Zero Trust architectures. We would be happy to discuss our submission and additional cybersecurity challenges of 5G in greater detail. For more information, please contact:

Katie Donnell
Associate Director, Government Affairs
kdonnell@paloaltonetworks.com

About Palo Alto Networks

Palo Alto Networks, the global cyber security leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cyber security partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

---

[1] For example, APIs should be designed with authentication, access control, activity monitoring (for suspicious activity), and encryption and integrity protection mechanisms can be applied where appropriate, such as to every exposed interface.