19 June 2020

Mr. Travis Hall
Telecommunications Policy Specialist
Office of Policy Analysis and Development
National Telecommunications and Information Administration
US Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Secure 5G RFC

Dear Mr. Hall:

I am writing on behalf of Juniper Networks regarding the above-captioned NTIA Request for Comments on the development of an Implementation Plan for the National Strategy to Secure 5G (Secure 5G Strategy). This initiative provides NTIA with a prime and timely opportunity to encourage investment in secure next generation networks. We recommend that NTIA coordinate a whole-of-government approach that prioritizes open standard-based and interoperable solutions as the means to achieving security.

By way of background, Juniper Networks is a California-based developer of high-performance networking hardware and software. Our product portfolio spans routing, switching, and security solutions. We proudly consider ourselves as secure networking partners to governments (at the national and local levels), major enterprises, service providers, and cloud providers around the globe.

We are pleased that NTIA has undertaken the initiative to seek input on how to implement the administration's National Strategy to Secure 5G. The Secure 5G Strategy, released in March of this year, is a promising framework for addressing the security challenges of next generation wired and wireless networks. We welcome the opportunity to partner with you to implement it and address each of your questions herein:

1133 Innovation Way
Sunnyvale, CA 94089
o +1 408 745 2000
f +1 408 745 2100
www.juniper.net

LINE OF EFFORT ONE: FACILITATE DOMESTIC 5G ROLLOUT.

We believe the government has two important roles for facilitating rollout of domestic 5G: that of convener and that of demand driver/customer. At the center of both roles is the promotion of open standard-based architectures.

One of the biggest obstacles to the development and deployment of widespread, secure 5G is widespread reliance on proprietary, legacy hardware and interfaces. It is well established that proprietary standards limit competition and innovation in the supplier market and increase costs; these are textbook characteristics of proprietary lock-in. End users that build networks with proprietary solutions can be locked into those suppliers (and the technologies they choose to provide) for the long-term, making it difficult for them to incorporate more innovative and secure technologies from alternative providers. The existence of open standard/open RAN initiatives allows new entrants to enter these markets and use cases and avoid existing technology barriers. Open standard-based 5G solutions are interoperable and permit operators to build networks from best-of-class products and services.

As a company that was established to support the most demanding needs of internet service providers, telecommunications providers, and the US government, Juniper always has been a proponent of open standard-based architectures. We are a member of several open standard bodies, including the O-RAN Alliance and the Open RAN Policy Coalition (ORPC). The O-RAN Alliance is a coalition of companies dedicated to the development of vendor-neutral hardware and software-defined technology based on open interfaces and community-based standards. The ORPC is a coalition of multi-national operators and suppliers advocating for government policies in favor of open RAN.

The government, as a convener on policy and standards development, can motivate 5G stakeholders to deploy open standard-based and interoperable solutions. NTIA, NIST, NSF, and Congress can have a primary role in this regard. In fact, all of these entities already have projects along these lines, including a current NIST project on 5G cybersecurity.

The federal government, as a customer, can drive demand of open standard-based protocols; on the supply side, this would encourage increased private sector investment. Many federal agencies still seek equipment that deploys legacy, proprietary protocols. When a class of customer with an annual IT procurement budget in the billions of dollars (e.g., the federal government) issues solicitations for legacy protocols, it sends a signal to suppliers that the

customer is not interested in deploying advanced solutions and thus discourages their development.

The government can overcome macro network barriers during the procurement process by the specification of open standards and open interfaces. This will increase competition, encourage innovation, and open the 5G market to new market entrants. Moreover, agencies that take advantage of competition and conduct market research that is open, transparent and brand neutral will better position themselves to build the most innovative and secure networks.

LINE OF EFFORT TWO: ASSESS RISKS TO AND IDENTIFY CORE SECURITY PRINCIPLES OF 5G INFRASTRUCTURE.

Juniper recommends that NTIA, as it is doing now, work collaboratively with stakeholders to assess risk and identify security principles that are core to 5G infrastructure. NTIA has a well-regarded track record of convening parties on all sides of issues to analyze complex issues and arrive at consensus decisions. The assessment of risk and identification of principles are no different.

We also must highlight that the federal government has several, disparate initiatives addressing the same issues. Recent laws focused on improving cybersecurity have (1) created the Federal Acquisition Security Council to coordinate federal policy, (2) required risk assessments of suppliers with foreign government affiliations, (3) developed a program for carriers to remove and replace untrusted suppliers, and (4) banned federal contractors from incorporating solutions from certain companies. At the same time, several agencies are proceeding with regulatory measures to (1) limit the export of technology, (2) impose strict cybersecurity requirements on contractors and subcontractors, and (3) subject private sector acquisition of IT products and services to government review. While we support the overarching goal of these initiatives (more secure networks), they do not appear as part of a coordinated strategy; instead, they seem responsive to highly-specific circumstances that then impose highly-specific and uncoordinated mitigations. A more coordinated strategy with industry, such as that envisioned by the Federal Acquisition Supply Chain Security Act of 2018, would advance the government's and industry's abilities to secure the Nation's networks.

LINE OF EFFORT THREE: ADDRESS RISKS TO U.S. ECONOMIC AND NATIONAL SECURITY DURING DEVELOPMENT AND DEPLOYMENT OF 5G INFRASTRUCTURE WORLDWIDE.

One of the most important ways for the federal government to address worldwide risks to security is to maintain support for international bodies, including standards development

organizations (SDO). Security cannot be achieved by one country acting alone or by focusing attention on one supplier or one country. The fact is that all nations are interdependent whether for political, economic, trade reasons. International organizations serve as a forum for governments and industry partners to raise and address differences and to arrive at consensus. Entities that choose not to participate in such forums are signaling their intent not to be partners in standardization and security.

Juniper is very active in standards bodies and industry organizations. To drive 5G innovation, we believe it is important to continue to drive access to spectrum, collaboration between industry and government to drive standardization in RAN, IP core/edge, and automation/operations interfaces for 5G networks. These goals cannot be achieved by the United States alone.

LINE OF EFFORT FOUR: PROMOTE RESPONSIBLE GLOBAL DEVELOPMENT AND DEPLOYMENT OF 5G.

As noted previously, we recommend that NTIA support federal government involvement in international standards bodies. The federal government's ability to influence global partners is enhanced when we participate in such forums. If we withdraw our representation, a vacuum is created that permits other countries, namely those with opposing views, to fill leadership roles and drive global technology decisions without us.

Thank you for your consideration of these views. Should you require any further information, please feel free to contact me at (571) 203-1908 or spgarg@juniper.net.

Sincerely,

Sampak P. Garg
Director of Government Relations

1133 Innovation Way
Sunnyvale, CA 94089

o +1 408 745 2000
f +1 408 745 2100

www.juniper.net