DELL Technologies

June 25, 2020

National Telecommunications and Information Administration
Attn: Travis Hall
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: The National Strategy to Secure 5G Implementation Plan (Docket No. 200521-0144)

Pursuant to the request for public comments issued by the National Telecommunications and Information Administration ("NTIA") regarding the National Strategy for Secure 5G ("Strategy") Implementation Plan ("Implementation Plan"), Dell Technologies Inc. ("Dell Technologies) respectfully submits this Comment Letter in response to the Strategy's four lines of effort: (1) facilitating domestic 5G rollout; (2) assessing the cybersecurity risks to and identifying core security principles of 5G capabilities and infrastructure; (3) addressing risks to United States economic and national security during development and deployment of 5G infrastructure worldwide; and (4) promoting responsible global development and deployment of secure and reliable 5G infrastructure.

General Comments

Dell Technologies commends NTIA for reviewing information on how to best facilitate the accelerated development and rollout of 5G infrastructure in the United States and internationally, as well as on how to lay the groundwork for innovation beyond 5G. The future of the economy and our communities depends on business and governments' ability to invest in a long-term digital transformation strategy. Dell Technologies believes the development and deployment of 5G plays a foundational role in that strategy. As such, we strongly support the U.S. Government and NTIA initiatives to build both the U.S. and technological allies' leadership in open and secure 5G ecosystem using three primary levers:

- Industrialize a secure, open-architecture, software-based 5G Open Radio Access Network (RAN) ecosystem for the U.S. and other developed economies, which includes a managed security framework
- Encourage adoption of Open RAN solutions by mandating specific platform requirements in appropriate federal solicitations and contracts
- Deploy federal economic incentives to stimulate the domestic development in the Telco cloud platform and build an application marketplace for the Telco cloud platform

I. Facilitating Domestic 5G rollout

In order to realize U.S. global leadership in 5G deployment, it is critical to enable the FCC to increase U.S. 5G spectrum allocation with focus on additional mid-band spectrum. In particular to maintain the December 2020 launch of the FCC spectrum auction for the mid-band frequencies in 3.7-3.98 GHz band and encourage the U.S. to quickly identify and bring to market

Dell Technologies • One Dell Way, Round Rock, TX, 78682 • 202.770.5011• DellTechnologies.com

additional mid-band spectrum for 5G. Additionally, the U.S. should develop a spectrum harmonization strategy and policies aligned with allied countries to improve 5G RAN economies of scale of which common frequency bands will drive higher Radio volumes and improve economies of scale for U.S. 5G solutions. The U.S. should continue to promote legislature that fosters efficient and cost-effective domestic 5G network rollout. Specifically, enhancements to policies that ease zoning restrictions and timely local decision making (shot clocks) to accelerate deployment timelines and lower deployment fee structure.

Fostering a vibrant R&D ecosystem

The next-gen network is not simply an evolution of 4G; it requires massive transformation, demanding new distributed architectures using software-defined networks. As governments around the world look to rebuild economies and invest in technology infrastructure, 5G gives all communities an opportunity to close the connectivity gap. The high speed, low latency performance of 5G will profoundly change the connectivity speeds, density and intelligence to consumers, enterprises and Internet of Things (IoT). However, in order to expand 5G and future wireless capabilities, we must also look to expand the current ecosystem which does not currently include a U.S.-based, at scale, 5G RAN solution company.

With the passage of the U.S. 5G Leadership Act, actions must be taken to build up a domestic 5G ecosystem that will allow for additional entrants into the market. To foster a competitive, domestic marketplace and guarantee our economic and national security, we need to bring new businesses of all sizes to the telecommunications industry and open 5G networks. This competition will create a diverse industrial base where all businesses can participate and bring new innovative solutions into our telecommunication networks as well as prevent vendor lock in that could lead to increased costs. To that end, we recommend the following actions:

Direct R&D and Industrialization funding to support the establishment of a U.S. Modern 5G ecosystem and trusted U.S. supply chain and technology innovation

While the U.S. continues to hold a large share in the of global R&D, the rest of the world has seen even greater increases in their investments in innovative technologies. As the U.S. looks to maintain its technological edge and build a trusted domestic supply chain, greater investment in 5G is necessary. We believe the following funding mechanisms are vital to the development of 5G in the U.S.:

- Fund 5G innovation based on open, interoperable standards, including prioritizing Open RAN in all funded 5G programs;
- Incentivize expansion of a trusted vendor radio equipment supply chain (including manufacturing) through R&D tax credits and other incentive vehicles;
- Incentivize expansion of trusted vendors developing open and interoperable RAN technology by utilizing public/private partnerships;
- Create a pipeline of R&D and industrialization funding for continued development of open and interoperable RAN; and
- Increase grant opportunities and grant amounts to qualified U.S. vendors;
- Design a program to incentivize investment and job creation in the U.S. by offering R&D credits and other incentives for network technology suppliers.

Establish and fund a 5G multi-vendor interoperability lab

Countries such as the United Kingdom and others in the European Union have developed programs that support local vendors and in-market 4G/5G solution integration. This approach can provide U.S. based compliance/interoperability facility as well as provide capital expenditure offset for the domestic 5G Open RAN ecosystem. The Federally funded 4G/5G Open Network and Open RAN interoperability labs could be oriented on 5G multi-vendor interoperability as well as 4G/5G network interop and handoff optimization.

U.S. Government IPR protection to U.S. 5G vendors

As U.S. 5G solutions expand in the U.S. and global market it is expected that an increase in IPR claims will develop. Enforce FRAND or similar concepts as well as the creation or adoption of a patent pool model to support domestic deployments and expansion to international allies.

Industrialization of a Robust Domestic 5G ecosystem

The U.S. Government plays a critical role in providing support for the R&D and industrialization of a robust domestic 5G ecosystem as well as providing funding and establishing requirements for 5G pilot programs and deployments. Together the R&D programs and the Federally funded pilot programs and commercial deployments can provide the necessary foundation to accelerate the 5G ecosystem through industrializing the supply chain, developing and hardening Open RAN technology and improving the performance and operability of Open RAN solutions. Mandating Open RAN solution in all Federally funded 5G pilots and deployments will help facilitate the transition to open systems and help identify challenges facing 5G deployments.

U.S. Government Procurement

Federal agencies should also establish procurement preferences for Open RAN technology. Examples include the following:

- Direct DoD to use its procurement authority to require testing or encourage deployment of 5G open and interoperable networks. Successful pilot programs from FY2020 and FY2021 should be expanded in both scope and scale as quickly as possible and transitioned into programs of record. Potential partners to expanding Open RAN pilots include: Defense Advanced Research Projects Agency (DARPA), Spectrum Forward Consortium, AFWERX, NavalX and Army Futures Command.
- Direct DOE to promote open and interoperable interface-based networks using its procurement authority for spectrum development projects through the Idaho National Laboratory, the Pacific Northwest Laboratory, and others.

Additionally, as the Department uses pilot programs for the development and deployment of 5G we believe the following recommendations serve as an opportunity to allow for additional entrants into the market and the creation of a domestic ecosystem:

- Incorporate open and interoperable RAN in some portions of its current and future 5G pilot programs both stateside and abroad (e.g., use a portion of its authorization to spend up to $275 million on Next Generation Information Communications Technology (5G) to deploy

Dell Technologies • One Dell Way, Round Rock, TX, 78682 • 202.770.5011• DellTechnologies.com

interoperable network technology in connection with implementation of Section 226 of the FY2020 NDAA).
- Accelerate these programs, ensuring Open RAN solutions are part of them, and allowing execution in the FY2020/21 time periods.
- Use its procurement authority to require testing or encourage deployment of 5G open and interoperable interface-based networks through the 5G to NextG solicitation (6-12 months out).

Secure funding for the removal and replacement of the unsecure technology

The development of future 5G networks is only one step in securing our communication networks. As recognized by the Secure and Trusted Telecommunications Networks Act, existing networks have security vulnerabilities that must be removed. We encourage the Administration and Congress to work together to fund this important initiative and aid small telecommunications networks in the removal of this equipment. We also recommend the inclusion of Open RAN as a technology option eligible for funding provided under program as well as extend the time period to complete the replacement to 18-24 months from 12 months to accommodate logistics.

Mandate that all USG funded mobile networks adopt U.S. 5G platform requirements

In order to facilitate a domestic, secure ecosystem, we recommend that agencies seek compliance with Open Network and Open RAN by 2022. Additionally, there are several 5G Federal funded programs in-flight or in planning that can be modified with modern 5G deployment requirement to further these goals as well. For instance, the Rural Digital Opportunity Fund and the 5G Rural America initiative proposed by the FCC are opportunities for integrating and mandating domestic 5G requirements.

II. Assess Risks to and Identify Core Security Principles of 5G Infrastructure

Security is a high priority for Dell Technologies. As wireless technology transitions to the 5G and beyond, comprehensive private-public sector partnerships should evolve existing security measures that have already been developed to adapt to existing networks. In addition, Dell Technologies recommends the following actions and concepts to create a telecommunications security environment that provides a supportable and sustainable basis for carriers to trust the hardware and software presented for deployment in their networks and ultimately materially improve our nation's security.

Factors for the development of core security principles for 5G infrastructure

Zero trust[1] or data-centric architectures put forth basic tenets or principles to secure modern infrastructure against today's threat landscape in which the primary concern is nation state sponsored threat actors. These tenets apply not only to core infrastructure, cloud, and edge, but also to the span of 5G technologies. The current threat landscape consists of sophisticated threat actors who will find the weak point in any system or within the ecosystem of the supply chain or connected devices. If a vulnerability exists, it will be identified, cataloged and used for exploits by a threat actor. As such, the principles of the zero trust architectural model build in safeguards to prevent an attacker from moving beyond their initial foothold, make it more difficult for an attacker to maintain that initial foothold, while enabling detection early in the Kill Chain[2] to minimize the amount of time an attacker remains on the network (dwell time).

While zero trust architectures continue to evolve, these tenets will remain steadfast and become increasingly pervasive to include trusted and verified infrastructure, isolating components/networks up and across the stack, consistent support for logging, strong encryption, and strong dynamic authentication. The verification of components, hardware and software, occurs at boot and continuously at run-time to provide an assurance of expected controls to more easily detect variances to prevent attackers from gaining a foothold. Components, devices, and people are continually authenticated to ensure only authorized access is permitted and changes in authorization are regularly enforced.

Useful and verifiable security control regime

Posture assessment has long been a goal of infrastructure security, but difficult to attain because of the required customization and maintenance of standards prior to attestation techniques being deployed. Attestation from a root of trust (RoT) and remote attestation finally make this goal feasible as the architecture and deployment scales. To ensure a verifiable control regime, standards to guide measurement and policy comparisons first attest hardware components are as expected, then iteratively provide attested verification throughout the boot process and during run-time. Attestation from a RoT has become standard practice with processes restarting or halting if expected values or policies are not met when attestation values are compared. Boot process verification has become standard process in recent years, with some systems enabling remote attestation. Run-time verification of these components has also emerged as standard practice for data center or cloud systems. NIST has established guidelines[3] for which specific control evaluations have been created in the Trusted Computing Group (TCG).[4] Similar requirements for 5G systems, including devices, should be established. The ability to collect this attestation information for centralized reporting is also evolving and is the most promising method to achieve verifiable controls in an automated and practical approach.
For 5G, this model must be expected of devices in addition to the use of technologies like the Manufacturing Usage Description (MUD) [RFC8520][5] where system profiles of expected behavior are established from a central point and distributed to all systems of a specific type.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf.
[2] https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.
[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf
[4] https://trustedcomputinggroup.org/work-groups/cyber-resilient-technologies/.
[5] https://tools.ietf.org/html/rfc8520.

This works well for systems or components with a small profile and can prevent DDoS attacks as well as detect and prevent compromises.

Stakeholder-driven approaches for consideration

Stakeholders should require intrinsically secure solutions that eliminate the need for add on products. The solutions should adhere to zero trust principles, where components are verified on a continual basis. It must be feasible to manage systems, therefore architectural patterns that scale with intrinsic security and automation should be considered required.

Adjusted commercial model to address security gaps

In order to scale security management, the market must pivot away from add-on products to intrinsic security. Incentives may be necessary to drive this shift to improve the overall security posture for 5G networks, which may result in market disruption for in-line or add-on products. Service offerings may be possible to support this shift and might include automated threat prevention, expected behavior pattern updates, and management of automated functions. Premiums might be considered for systems, devices, or applications that do not require add-on security products.

III. Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide

To secure a broad diversity of wireless equipment suppliers, Dell Technologies recommends the U.S. cooperate with trusted foreign countries to provide effective risk-mitigation strategies as well as development and deployment of viable alternatives to high-risk vendors, such as O-RAN, as described above. Dell Technologies urges that any efforts to build a market for more secure 5G equipment should also ensure companies can continue to innovate, in addition to encouraging other countries to invest in 5G security.

Domestically, the relevant agencies should coordinate with private entities to help mitigate supply chain risk. One example of existing coordination efforts in this area includes the Information and Communications Technology Supply Chain Risk Management Task Force, managed by the Department of Homeland Security.[6] This and future public-private partnerships will effectively develop recommendations to identify and manage risk in the global supply chain. Future task forces should provide for secure information sharing systems to manage cyber and other related threats to 5G infrastructure. Ultimately, a well-coordinated inter-agency partnership with private entities is critical to providing and maintaining an effective supply chain risk management plan.

IV. Promote Responsible Global Development and Deployment of 5G

[6] Cybersecurity and Infrastructure Security Agency, *Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force* (March 5, 2019), https://www.cisa.gov/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force

To effectively promote a diverse, competitive supply chain of trusted, secure, open and interoperable technologies, the U.S. should employ the following short- and long-term efforts.

- The establishment of NIST security and resiliency guidelines for 5G connected systems that could result in specified control measurements, such as the work for firmware resiliency could be used to provide consistent and secure equipment.
- Leverage U.S. international funding agencies (e.g., EXIM, DFC, USAID), and the State Department, to encourage Open RAN solutions in wireless projects that will result in the deployment of open interoperable network equipment from trusted vendors and service providers.
- Prioritize Open RAN advancement in EU, Indo Pacific Strategy with enhanced funding
- Encourage deployments in other markets, including India and Brazil.
- Fund international collaboration such as joint R&D programs.
- Coordinate with like-minded countries to adopt similar policies such as: (i) Supporting open and interoperable RAN solutions from trusted vendors and service providers with their government funding sources; and (ii) Implementing the widely accepted Prague Proposals calling for “open, interoperable, secure standards, and industry best practices to promote a vibrant and robust cyber security supply of products and services.”

U.S. companies can benefit from a substantial government investment in 5G infrastructure as well as research and development grants. As previously stated, the U.S.-based secure Open RAN solution is a viable alternative to foreign and proprietary RAN solutions for global deployments. The secure Open RAN solution has clear advantages over proprietary RAN solutions. In addition, the Open RAN platform is software-defined and has open interfaces that allows for multi-vendor interoperability. Furthermore, through an open radio interface controller, application programming interfaces for third party application developers can take advantage of radio information supporting low latency 5G applications such as artificial intelligence and machine learning based automation and optimization. Overall, Open RAN platforms scale with an ecosystem of third-party developer innovation partners unlike closed proprietary RAN solutions.

Conclusion

Dell Technologies appreciates the opportunity to comment on NTIA’s Implementation Plan. As NITA considers the Strategy’s Implementation Plan, Dell Technologies urges NTIA to deploy a flexible plan that is composable and scalable to the needs of the evolving 5G network. Importantly, there should be a focus to incentivize the establishment of a trusted U.S. supply chain and technology innovation through government procurement and research and development. Ultimately, investment in Open RAN technology, global partnership in technology, and public-private coordination in supply chain security will enable the successful development and deployment of 5G infrastructure in the United States and internationally. If you have any questions, please reach out to Kristen Mattern (Kristen.Mattern@dell.com).