July 28, 2020

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

Re: Comments of Dell Technologies, Inc -- Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers (Docket No. 200609-0154)

Dell Technologies Inc. ("Dell Technologies") respectfully submits this Comment Letter in response to the request for public comments issued by the National Telecommunications and Information Administration ("NTIA") issued on June 12, 2020 (85 FR 35919) regarding the sharing of supply chain security risk information with trusted providers of advanced communications service and suppliers of communications equipment or services. Dell Technologies encourages the NTIA's and U.S. supply chain policy generally to prioritize U.S. managed contents to ensure global supply risks are effectively mitigated.

Trusted Providers and Suppliers

Dell Technologies supports the definition of "trusted providers and suppliers" under Section 8 of the Secure and Trusted Communications Network Act of 2019, which excludes the sharing of information with entities "not owned by, controlled by, or subject to the influence of a foreign adversary."[1] However, there needs to be greater clarity on delineating the difference between foreign "trusted providers and suppliers" and U.S. technology companies. Dell Technologies emphasizes the need to prioritize domestic technology companies as trusted providers and suppliers as a U.S. company's oversight of the supply and manufacturing ecosystem contributes to both our national and economic security.

The commercial success of 5G is dependent on it being integrated with an enterprise environment. However, every company has their own supply chain process and, as such, we must ensure those that contribute to our critical infrastructure abide by similar business processes and reporting requirements. This will ensure that these networks are in compliance and that everyone abides by a standardized command and control system to prove their compliance. At Dell Technologies, a demonstrated commitment to transparency, collaborative leadership, innovation, and empowering team members and suppliers is vital to our efforts to improve the sustainability of our supply chain. We continuously monitor our suppliers' adherence to our standards and work with them and other stakeholders to address potential risks.

Due to the critical nature of 5G networks to our overall telecommunication networks, one major factor that needs to be considered in determining supply chain risk is place of manufacturing. The U.S. does not have an at scale provider for all components of 5G networks. As a result, IT hardware manufacturers are highly reliant on global suppliers for vital components to our telecom networks. While manufacturing companies are diligent in mitigating known risks in their supply chains, they may not be fully aware of subtle risk in each element embedded within the multiple subsystems in a typical final solution. Additionally, while the lifetime of telecommunication systems can last over a decade, there appears to be limited consideration of the overall viability and sustainability of manufacturers themselves in the discussion of long-term

supply chain risks. Yet, because of reliance on global entities, providers have little visibility into the viability of their manufacturers and whether they will still exist years down the road to service the networks and replace key components. Thus, we recommend that NTIA share such risks with providers and, as a result, mandate the U.S. buildout of 5G systems and future generations should utilize U.S. managed subsystems and content including computer platforms, virtualization technology, cloud software, networking technology, optical technology, and antenna, among other technology. This will not only give an assessment of existing risks in their supply chain and increase visibility, but it will also allow them to become less reliant on foreign entities and create a healthy ecosystem that will provide supply chain assurance in the years to come.

The broad technology ecosystem, which includes hundreds of U.S. companies and innovators, are increasing their focus on 5G to provide content for these systems. In order to accelerate development and rollout of 5G infrastructure domestically, U.S. government policy needs to support U.S. technology companies as priority trusted providers and suppliers. The shift to U.S. content is critical not just for the purpose of building 5G telecommunication systems but rather for the impact on consumers of those systems and private 5G systems that will exist in every major industry within the U.S. economy. The lack of a secure supply chain, U.S. technology, and control over the intellectual property rights of the 5G ecosystem by U.S. companies will introduce significant strategic, economic, and political risk to the communications industry. The impact of these deficiencies goes beyond just mobile connectivity.

The scale of 5G requires intrinsic security with validated assurance that can be completely automated, in support of assuring a secure and trusted supply chain. Following the tenets of NIST's Zero Trust Architecture [NIST SP 800-207] as applied to infrastructure, hardware is verified, and components upon boot and at runtime are compared to 'golden policies' and measurements. If a policy or measurement is not met, remediation is required to ensure a resilient supply chain. The components are verified in sequence on boot and may be chained from dependencies through attestations from a root of trust (RoT). The policy comparisons may be updated by the manufacturer when patches or updates are issued, and the attestation may be collected into central repositories providing posture assessment for all systems and components of infrastructure in the supply chain through remote attestation technology

Information Sharing Policies and Procedures

Dell Technologies supports NTIA's plans to structure the information sharing program to promote the flow of risk information from the government to small and rural providers and suppliers. In addition to small and rural providers and suppliers, Dell Technologies urges the U.S. to provide a vehicle for the broader U.S. technology ecosystem to coordinate with the government on effective risk-mitigation strategies and deployment of viable alternatives to high-risk vendors. Dell Technologies recommends that any efforts to build a market for more secure 5G equipment should also ensure companies can continue to innovate. Information sharing models should shift to automate deployment for threat mitigation sourced from the vendor to enable immediate mitigation from point of vulnerability disclosure, in order to serve customers of all sizes and reduce the need for experts at every location.

While sharing information with providers of all sizes is helpful, enabling immediate remediation controls through technologies such as the Manufacturer Usage Description (MUD) [RFC8520] will have a greater impact in today's threat landscape. Sophisticated threat actors are actively deploying exploits against "day one" vulnerabilities. As such, patches must be contained to the applicable components following zero trust isolation principles to allow for centralized testing

from the vendor to ensure minimal impact with immediate deployment. Similarly, mitigation methods such as those possible using MUD can be used to provide immediate protection from the vendor to improve the scale of managing security. Vendors, including those using libraries with identified vulnerabilities, should be included in the responsible disclosure process to ensure patches for long-term remediation and short-term mitigation methods may be automated. This will eliminate delays that can occur with manual processes and can address not only allowing expected ports and protocol access, but also updating expected behavior patterns to prevent exploits. Similar patterns that scale from the manufacturer or software provider are recommended to thoughtfully consider small and rural providers and to reduce the resource requirements for any provider.

Conclusion

Dell Technologies appreciates the opportunity to comment on this Notice and supports NTIA's efforts to gather feedback on the best ways to facilitate the sharing of security risk information with trusted providers of advanced communications service and suppliers of communications equipment or services. Dell Technologies urges that U.S. policy related to communications suppliers and providers recognize the existing and potential U.S. managed contents that can be used to build 5G systems and future generations. Further, Dell Technologies encourages the prioritization of U.S. based systems and subsystems to build out a secure and reliable 5G infrastructure.

[1] Secure and Trusted Communications Network Act of 2019, § 8(c)(4).