Testimony of

Michael Murphy

Chief Technology Officer

Americas

Nokia

Hearing On

“5G Supply Chain Security: Threats and Solutions”

before the

U.S. Senate

Committee on Commerce, Science, and Transportation

March 4, 2020

Chairman Wicker, Ranking Member Cantwell, and members of the Committee, on behalf of Nokia, thank you for the opportunity to testify today.

Nokia appreciates the leadership of this Committee, Congress, the Federal Communications Commission (FCC), and the Administration in securing U.S. communications networks. In this testimony, I want to discuss several topics.

- First, given recent congressional action regarding the critical need to move forward in assisting small carriers with removing untrusted vendor equipment in their networks, I will outline several issues Congress and the FCC must keep in mind to ensure that the removal occurs without a negative impact on carriers and the communities they serve.
- Second, an important element of ensuring a secure supply chain for communications equipment is guaranteeing that the trusted suppliers already providing equipment to the U.S. market can compete at a global scale and on fair terms. I will share Nokia's perspective on the current global marketplace and some challenges that are the result of advantages extended to Chinese suppliers that are not available to other suppliers and how that can be mitigated to ensure a level playing field for trusted suppliers.
- Finally, I will highlight several of Nokia's leading security and supply chain activities, including design for security and supply chain validation, and why we believe they result in trustworthy networks. I will also comment on how new U.S. actions on supply chain security should recognize practical timelines to ensure execution success.

About Nokia:

Nokia is the industry’s only global supplier having an end-to-end portfolio of network equipment, software, services and licensed technology. Our customers include communications service providers whose combined networks support 6.1 billion subscriptions, and our enterprise customers have deployed over 1,000 industrial networks worldwide. We transform how people live, work and communicate. We are the only telecommunications equipment provider listed in Ethisphere’s 2020 Honoree list of ethical companies.

Nokia has a massive presence in North America with more than 11,000 employees, the bulk of those in the United States. We have 28 sites including five major innovation hubs of which four are in the United States: Sunnyvale, CA; Dallas, TX; Naperville, IL; and Murray Hill, NJ the site of the iconic Nokia Bell Labs, recipient of 9 Nobel Prizes. There are also two major Nokia data centers in the U.S., one in Plano, TX and the other in Chicago, IL. In addition, SAC Wireless, a Nokia subsidiary, has 21 sites in the United States. SAC offers turnkey services to support major network builds and upgrades for 4G, 5G, Small Cells and FirstNet. Those services include site selection and acquisition, engineering, construction, optimization, maintenance and end-to-end program management.

Nokia has been a leader in every generation of wireline and wireless communications to date and continues that leadership in 5G. The race to innovate never stops. In fact, even as we continue to roll out the earliest 5G networks, our work on 6G has already begun at Bell Labs.

Removal and Remediation of Equipment Provided by Untrusted Vendors in U.S. Rural Networks

Throughout the FCC’s secure supply chain proceedings, Nokia provided technical input on the strengths and weaknesses of networks with respect to their inherent security and how a secure supply chain could be created by using our own company's internal governance as examples.

Now, given the FCC's decision to require removal of equipment from certain vendors, Nokia would like to offer additional perspectives on what the FCC and Congress should bear in mind before prescribing the final replacement guidelines and funding criteria. That advice, as I outline herein, is that flexibility in timing and technology neutrality will be essential if this effort is to be successful. Executed well, this effort can also help in the U.S.'s drive towards 5G leadership.

Flexibility in timing:

The FCC correctly recognized during its rulemaking process that a funded reimbursement program should be implemented before requiring recipients that receive universal service fund support to remove and replace covered equipment from their networks. Congress has taken the first critical step by passing the Secure and Trusted Telecommunications Networks Act.[1] Nokia believes that several provisions of the Act are prudent, particularly the provision granting discretion to the FCC to extend the time allowed for impacted carriers to replace covered equipment from one year, by up to an additional six months, and the directive for the FCC to remain technology neutral in establishing the list of recommended replacement equipment. The following provides some detail on why we support those provisions.

Nokia completed more than 60 major swaps in the last three years, including the largest ever done, replacing 75,000 base stations in both the Verizon and AT&T networks following our acquisition of Alcatel-Lucent and the transition to a new product platform. Those projects

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, and Order, WC Docket No. 18-89, FCC 19-121, ¶ 122 (rel. Nov. 26, 2019) ("*Order and FNPRM*").

required removal and replacement while also maintaining service continuity and service quality. That is -- and should be -- the expectation of swap activities for all impacted carriers in this context. Based on those past experiences, Nokia can attest that these efforts require careful planning, are network specific, and the times required vary significantly from project to project. Network size is not the only factor affecting timelines. For example, new product variants or features may be required for unique spectrum combinations or to match customized capabilities provided by the previous vendor.

Beyond routine timelines, ongoing large 5G builds are creating a shortage of qualified tower crews. In fact, despite Nokia having the largest in-house field service team in the U.S., we still see a dearth of crews to meet 5G demands in 2020 and into 2021. Small rural markets covering vast rural landscapes with shortened climbing windows during winter months only exacerbate the issue. We appreciate the leadership of Senators Thune, Tester, Moran, Peters, and Wicker in introducing the Telecommunications Skilled Workforce Act to help address this gap.

In short, our view is that flexibility in timelines are a necessary practical reality, and thus extensions to the current one-year proposal will likely need to be granted liberally.

Flexibility in technology:

During the rulemaking process, the FCC proposed "to make available reasonable replacement costs for the equipment and services produced and provided by covered companies . . . ."[2] and asked whether recipients of universal service funding should be "allowed to seek reimbursement for technology upgrades to their networks . . . ."[3] Nokia noted to the FCC that carriers replacing equipment need to have the freedom to buy solutions that are not just "like for

[2] *Id.* ¶ 137.

[3] *Id.*

like," due to the unique times we are in (that is, in the midst of a 4G to 5G transition, the drive towards more open systems and virtualization). All of these play a role in what a rural carrier should, or should not, do in removing and replacing a supplier. The following provides Nokia's recommendation on these competing and complex topics.

Regarding "like for like," Nokia is and will continue to offer such solutions to all impacted carriers when they are available, appropriate and cost-effective. However, a significant part of Nokia's portfolio sold today supports both LTE and 5G through software upgrades. Replacing impacted carriers' equipment with older generation "LTE only" hardware could burden rural communities with avoidable near-term high 5G upgrade costs. A potential way forward is to offer "5G Ready" hardware but costing only the LTE components. Putting it another way, supporting "like for like" at the service level, but not necessarily at the hardware level. This would help mitigate the risk of gold plating and potentially help accelerate 5G in rural communities, thus supporting the U.S. drive towards nationwide 5G leadership. In short, there are no downsides.

In addition to avoiding being overly prescriptive on replacing "like for like," the FCC should also not condition funds on any prescriptive technology mandates. No specific technology, network configuration, or other similar mandate will be a one-size fits all solution to all network deployments. For this reason, Congress was wise to direct the FCC to implement a list of potential replacements that is technology neutral. At the same time, a recently introduced Senate bill suggests restricting any money for replacement on the condition that the relevant carrier must develop and submit a plan certifying that it will migrate to an open solution within seven years. While the intent of that bill is to encourage U.S. based 5G entrepreneurship, its timing brings with it some practical challenges.

The reality is that fully compliant open interfaces as specified by the ORAN Alliance, the most relevant in this context, have not been deployed anywhere in the world yet. These are new grounds for the industry. In fact, it is uncertain whether the most critical interface specified by ORAN will be deployed widely, as alternatives are already being proposed by several contributing, significant members. Likewise, virtualization, an orthogonal technology to ORAN, that can also facilitate open systems, has only been deployed by one carrier globally in a 5G Radio Access Network. In short, there is limited maturity in both ORAN and Radio Access Network virtualization. For this reason, Nokia believes that putting these burdens on rural carriers, the least capable of being early adopters, would be unreasonable and should not be a pre-requisite for federal funding to replace their existing equipment, at this time.

The Challenging Marketplace for 5G

Speculation about "the Race to 5G" and anxiety about which countries will lead and which vendors will prevail has been a staple of public commentary for the last couple of years. Much of that commentary and anxiety has suggested that non-Chinese vendors are not capable of matching the breadth or quality of products offered by Chinese suppliers and, as a result, would not succeed. While that argument is incorrect, there are areas of concern that need to be addressed.

The U.S. was the first country in the world to launch 5G in the fourth quarter of 2018, followed by more significant launches in April of 2019. The U.S. was also the first country in the world to launch 5G based on mmWave. The first to launch 5G on low band frequencies, nationwide. The first to deploy a virtualized solution. And the U.S. will also be the first globally to launch what is called a Standalone 5G core network and the first to launch a technology called Dynamic Spectrum Sharing or DSS, allowing 5G and 4G to be deployed on the same spectrum.

These firsts have and are being done by Nokia, Ericsson and Samsung. So, it is factually incorrect to say non-Chinese vendors are incapable of leading in 5G.

That does not, however, mean that the marketplace is without challenges. Policymakers should note that the pressure on many global wireless operators to reduce capital and operations costs, if very high, even as they deploy 5G networks, is very high. Against this backdrop, government programs including export credit agencies play a very significant role in coloring the attractiveness of supplier pricing. China has made aggressive use of its development bank and other programs to support its indigenous suppliers. Other nations have been far more reserved. For example, the U.S. Export Import Bank has not focused on telecommunications infrastructure projects in many years.

The payment terms being offered by Chinese suppliers suggest the underlying financing mechanisms, while legal, are neither consistent with commercial norms, nor available to competitors from commercial banks. We believe this is an approach that is common across many markets now based on requests from some of our customers to match these lengthy, low-interest payment terms. We raise these lawful finance mechanisms to ensure that Congress and the Administration know that they have tools available today to make a considerable difference in the competitive balance in the coming years through existing institutions.

The U.S. Export Import Bank and the recently renamed International Development Finance Corporation could potentially provide billions of dollars of grants, direct loans, loan guarantees, and insurance to exporters of 5G technology with its origins in the U.S, including to Nokia. Fortunately, there is movement in this direction now that reauthorization has been completed and the Administration appears to support moving forward as well. I encourage Congress to express its support for using these important programs to support trusted suppliers and to help them compete on a more level playing field internationally.

An additional challenge is that the Chinese telecommunications market is massive and dominated by domestic suppliers that collectively provide more than 70 percent of the equipment for LTE networks, a figure that is likely to go higher in 5G. That places Chinese suppliers in a position whereby they can spend massively on R&D and use that depth in foreign markets. Policymakers here in the U.S. and other nations that want to ensure a diversity of suppliers should work to coordinate their own R&D support programs might be utilized and coordinated to support a level playing field. To date, much of the R&D spending in the U.S. has been in support of foundational research through funding of incubators via the National Spectrum Consortium and US Connect. The recent Senate Intelligence Committee bill authorizing significant funding for research on network virtualization is an additional opportunity to provide essential research support. These are well designed efforts showing the potential for promising returns, but they are ultimately insufficient in scope and resource level. The missing components are support for further 5G product development, 6G foundational research, and support generally for creating new manufacturing and industrial base development activities in the U.S.

5G Security Planning and Nokia's Supply Chain Practices and Policies

I would like to turn now to the topic of 5G readiness and security. It has become widely understood that 5G will enable advanced, new use cases supporting critical services such as autonomous driving, factory automation, connected healthcare and others. These, combined with an architectural approach that includes virtualization and distribution, increases the inherent risk and potential damage caused by bad actors on 5G networks. Putting it another way, as 5G expands beyond smartphone users, and IoT devices start to play a larger role, the network attack surface increases. This has given rise to concerns about whether 5G is “ready” from a security perspective. We believe it is for several reasons.

First, learnings from LTE networks and the vulnerabilities encountered in them have been addressed by improved security mechanisms in 5G standards as specified by 3GPP. For example, in 4G networks, the identify of users is often transferred “clear” across the air interface. This has allowed “IMSI hackers” to capture user identities and use them maliciously. This has been corrected in 5G through encryption of user identities. At this level, 5G is a significantly more secure system. Second, in addition to improving interface level security, 5G also introduced network wide security through the concept of secure, virtual “slices” across networks that cannot be breached by users in other slices. Visualize a government “slice” across a public network, that is protected and unreachable by users in a public smartphone slice.

However, even with these improvements, the reality is that bad actors could still infiltrate a 5G network. In other words, you still must trust suppliers to not act maliciously even with improved, standardized approaches to security. In that regard, Nokia does not support the view that either product or geographic isolation are effective. A breach in one part of a network could extend to other parts of the network. For this reason, Nokia believes the final and most important element of a secure system, comes from the governance models, ethical behavior and product development processes that suppliers demonstrate and apply. And here I would like to provide Nokia as an example.

One of the reasons for Nokia being on Ethisphere’s ethical honoree list comes from internal governance that mandates both corporate and personal ethical behavior. Training in ethics and reporting of unethical behavior is mandatory for all employees and is a prerequisite for employment with zero tolerance.

At the product level, Nokia systemically ensures that the products we deliver are secure through a Design For Security (DfSec) governance model that involves security testing of all product releases and continuous monitoring of all software components used in our products for vulnerabilities. Product teams have structured processes and enforced timelines for how any uncovered vulnerabilities must be handled and communicated to affected customers. To ensure our own products are secure during this process involves strict guidelines related to coding, hardening, testing, and updates. Processes we expect of 3rd party suppliers as well. Transparency and a governance model for corrective action are part of how we deliver products.

Finally, Nokia monitors a number of networks through a Threat Intelligence Lab. Results from that lab allow us to understand and deliver updates to customers to proactively prevent wider issues.

I hope that this information provides a meaningful basis for U.S. consideration about future supply chain activities. It is critically important that policymakers understand what is actually done today to ensure component security, product security and post-sale security support before prescribing new regimes for testing or certification that could impose costs on your trusted suppliers without necessarily providing a security dividend. And that is where a supply chain security strategy really should begin, careful assessment of known risks and current industry practices. Actions the U.S. might consider should draw from areas only where gaps are perceived.   In helping industry to be a constructive partner in this process, Nokia recommends the following:

- Identify best practices in design for security, supply chain validation and post-sale support and encourage the adoption of those practices ;

- Rather than focus on countries of origin for component sourcing or manufacturing, specify the components or activities that give rise to the risk of exploitation or manipulation. Not all components and products create risk. Narrowing the focus to specific components or products with risk will assist suppliers in making critical and cooperative decisions with governments about supply chain activities.

Thank you again Chairman Wicker, Ranking member Cantwell and members of the Committee for the opportunity to testify here today.