Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, DC 20230

In the Matter of	)	
	)	
The National Strategy to Secure 5G	)	Docket No: 200521-0144
Implementation Plan	)	RIN: 0660-XC047

COMMENTS OF NOKIA

Nokia submits these Comments to the National Telecommunications and Information Administration ("NTIA") in response to the above-captioned request for comments on development of a national strategy to secure 5G.

I. ABOUT NOKIA

Nokia offers unparalleled leadership in the technologies that connect people and things. Nokia is leveraging its strengths to create a new type of network that is intelligent, efficient, and secure, and which will serve as a critical enabler of many capabilities and use cases associated with 5G and the Internet of Things (IoT). We are weaving together the networks, data, and device technologies to create the universal fabric of our connected lives. Nokia brings together, in one company, mobile broadband with fixed line access, and the underlying IP routing and optical technology that connects them.

Nokia has been a major part of the U.S. wireless ecosystem from the beginning, providing networks and devices through multiple generations and evolutions. Our network solutions securely connect over 90 percent of the U.S. population and are supported by more than 10,500 U.S.-based employees. With five U.S. R&D Centers and the world-renowned Nokia

Bell Labs, we are deploying 5G networks and cloud-native software with all major U.S. communications service providers and providing mission-critical private networks for U.S. enterprises and public sector agencies.

II. RECOMMENDATIONS FOR LINES OF EFFORT ONE, TWO AND FOUR

A. Line of Effort One: Facilitate Domestic 5G Rollout

1. How can the United States Government best facilitate the domestic rollout of 5G technologies and development of a robust domestic 5G commercial ecosystem?

The U.S. government has taken a number of steps already to facilitate the introduction of 5G. Indeed, based on the innovation cycle that has historically required 10 years for the next "G," most predicted 5G deployments to begin in the 2020s. Buoyed by forward-thinking U.S. policies, however, the first deployments of this new generation of wireless technology reached U.S. shores in 2019. The U.S. is not alone in its efforts to accelerate the next generation of wireless, with numerous countries vying to win the "Race to 5G." While early U.S. policy action helped the country establish an impressive early foundation for future deployment this is not time to get complacent. Below we discuss Nokia's recommendations for facilitating 5G based on the three pillars of the Federal Communications Commission's ("FCC's") "5G Fast" plan – spectrum, infrastructure policy, and modernizing regulations. Each of these pillars must be aggressively pursued for a domestic U.S. ecosystem to thrive.

Spectrum. Spectrum is the life blood of 5G, which benefits from large channel sizes far beyond prior generations of wireless. Additional radio spectrum for mobile networks needs to be allocated and put into use quickly to meet the increased capacity and coverage demands of 5G. While U.S. operators currently hold significant spectrum, and have begun 5G deployments in a range of bands including 600 MHz and mmWave bands, there are questions

whether the amount of spectrum available, and mix of bands, will allow the evolution to fully capable 5G that Nokia expects will have data rates upwards of 20 Gbit/s. The piece that the U.S. still must lock into place is mid-band spectrum for 5G.

Nokia has been a consistent voice promoting mid-band spectrum for commercial wireless services, and in particular, throughout the entirety of the 3 GHz band -- in the 3.1-3.55 GHz range, the 3.55-3.7 GHz range, and the 3.7-4.2 GHz range. Each of these ranges pose their own unique challenges with respect to incumbent use cases requiring different approaches to unlock their promise, but the value of this full range of spectrum cannot be overstated. As the FCC has repeatedly recognized, ". . . mid-band spectrum is well-suited for next generation wireless broadband services due to the combination of favorable propagation characteristics (compared to high-bands) and the opportunity for additional channel re-use (as compared to low bands)."[1]

The technical propagation benefits lead to another benefit of this mid-band spectrum range. Base stations in the 3 GHz range can leverage existing deployment footprints to a larger extent than equipment for mmWave bands, resulting in lower site acquisition costs and shorter timelines for deployment. Equipment in this spectrum range will be incorporated in small cell deployments to increase capacity close to the user, and also will be deployed on existing macro-towers to improve coverage over larger areas. As such, the spectrum propagation characteristics of the 3 GHz spectrum bands will likely result in lower deployment costs and faster deployment when compared to the mmWave spectrum bands recently auctioned by the FCC.

[1] *Facilitating Shared Use in the 3.1-3.55 GHz Band,* WT Docket No. 19-348, FCC 19-130, ¶ 9 (rel. Dec. 16, 2019).

The U.S. market eagerly anticipates auctions in 2020 of two portions of the 3 GHz range: (1) the 3.5 GHz auction, up to 70 MHz of spectrum shared with Federal incumbents, scheduled for July 2020; and (2) the 3.7 GHz band auction, 280 MHz of spectrum, scheduled for December 2020. The timelines for these auctions must not slip. Indeed, key countries recognized mid-band spectrum as the workhorse for 5G and are ahead of the U.S. in auctioning and assigning spectrum in the 3 GHz range to terrestrial operators. Australia, Finland, Germany, Italy, Ireland, Japan, Kuwait, Latvia, Mexico, Oman, Qatar, Saudi Arabia, South Korea, Spain, the United Arab Emirates, and the United Kingdom are among countries that have already auctioned mid-band spectrum for 5G, not to mention China's allocation of large blocks of spectrum for 5G.[2] It is through these first-to-market, robust spectrum initiatives that these other countries seek to lead the Race to 5G.

The U.S. should also maximize the spectrum opportunities in the lower 3 GHz range currently under consideration by NTIA and the FCC. The U.S. must not settle for the relatively small allocation of spectrum (100 MHz of shared spectrum) currently highlighted by NTIA for shared use.[3] The entire 3.1-3.55 GHz range must be on the table, with potential commercial exclusive licensed use under study for at least some portion of that range. Such bold actions will be necessary for the U.S. to stay competitive on a global scale. Nokia advocates for allocating as much spectrum as possible in the 3 GHz range to terrestrial wireless, which would facilitate multiple carriers achieving true 5G performance in mid-band spectrum ranges.

As a final note on spectrum, 5G relies heavily on backhaul. 5G will require far more wireless base stations than prior technologies to reach its full potential, but most

---

[2] *See id.,* Statement of Commissioner Jessica Rosenworcel.

[3] *See, e.g., Technical Feasibility of Sharing Federal Spectrum with Future Commercial Operations in the 3450-3550 MHz Band*, NTIA Technical Report 20-546, January 2020.

prospective 5G base station locations are not connected to fiber, the gold standard for backhaul. As such, while policymakers should promote proliferation of fiber backhaul, they should also ensure that there is sufficient spectrum and the right policies in place to allow for wireless backhaul solutions. As one example, Nokia is currently leading the charge for rule changes in the U.S. 70/80 GHz band to allow for smaller, lighter wireless backhaul equipment in that band, which will facilitate more rapid 5G deployment to U.S. cities and towns.[4] Similar rules facilitating 5G wireless backhaul in the 70/80 GHz band are already in place in numerous countries. These types of policies are key to U.S. competitiveness in 5G.

Infrastructure Policy. 5G requires many more base stations to meet the performance needs of future applications. These dense networks will be deployed as heterogeneous networks, combining macro sites with smaller base stations that will collectively utilize a range of radio access technologies including LTE-A, Wi-Fi and any future 5G technologies. The FCC and the Administration already have taken substantial action to reduce the disparities in local siting rules for infrastructure.

For example, in 2018 alone the FCC issued major reforms estimated to save our country billions of dollars in red-tape spending by updating Federal environmental and historic preservation rules and then state and local siting policies, clarifying reasonable fees and timeframes for government review of applications to site small-cell infrastructure.[5] Just this month, the FCC clarified its rules governing local review of tower modifications to guard against

[4] *Modernizing and Expanding Access to the 70/80/90 GHz Bands*, WT Docket No.20-133, et al., FCC 20-76 (rel. June 10, 2020).

[5] *See, e.g., Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment,* Declaratory Ruling and Third Report and Order, 33 FCC Rcd 9088 (2018); *Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment,* Second Report and Order, 33 FCC Rcd 3102 (2018).

unwarranted delays. These reforms have the potential to free substantial capital for expanded network investment.

U.S. policymakers must be vigilant, however, in monitoring whether 5G is excluded from certain communities because of local government siting policies. Nokia appreciates the FCC's actions thus far, but real-world experience demonstrates that challenges still remain to rapid deployment of wireless infrastructure due to state and local siting processes.

Reforming siting regulations and revising rules and increasing access to federal lands have been mainstays of the effort to improve the pace of infrastructure deployment. There are additional opportunities that Nokia recommends to Congress and the Administration that should be pursued, particularly through any proposed infrastructure funding legislation. Policymakers should focus on a "smart" framework that looks to ease the deployment of infrastructure by, for example, 1) ensuring new roads and highways include conduit to facilitate future fiber deployment, 2) ensuring newly constructed and replacement bridges include sensor technologies and, where appropriate, attachment points for future radio cell deployments, and 3) incentivizing utilities deploying new facilities to similarly include sensors and attachment points. These actions will greatly accelerate the move to improved efficiency and cost of maintaining connected infrastructure and provide additional future deployment platforms for mobile wireless services.

Modernizing regulations: Network evolution requires innovation, which is fueled by the substantial commitment of financial resources regularly made by operators and infrastructure vendors into new research and development. It is critical that U.S. 5G deployments, R&D, and 5G test beds be sufficiently advanced that the U.S. continues to be the global center of gravity for network and edge innovation. This Administration should be

commended for advancing light-touch policies aimed at maximizing value creation and innovation for service providers and end-users.

The current Administration's commitment to light-touch regulation of broadband has fueled continued investment in U.S. networks and continuation of that policy is critical to the U.S. keeping pace as the global leader in wireless technologies. Mobile operators will invest in critical capacity and capability, but are discouraged from doing so when the return on that capital deployed into infrastructure does not recover the cost. The ARPU and ROCE metrics are therefore a bell-weather for the investment environment because they are proxy measurements for the ability to monetize marginal investment in the network.

This is a key reason that proponents of a return to utility-like regulation of broadband networks miss the mark, and increasingly so for 5G. Under a regulatory framework in which all traffic must be treated the same, and all consumers purchase their service via pre-packaged plans with no ability to differentiate service to willing users or application and service providers, the entire burden for funding research and development and network construction falls on consumers because they are the one and only source of revenue to the operators. At the same time, broadband providers are restricted from exploring revenue sources that could alleviate the burden consumers carry for funding network upgrades and expansions.

Robust R&D in the infrastructure sector requires healthy monetization and investment by operators in network upgrades and improvements. In turn, the evolution of networks through the availability of aggregation technology, small cells, caching and other emerging technology further enables edge companies to develop data hungry applications of increasing sophistication to meet consumer demand.

Beyond the features and services that consumers actively seek, there will also be certain features that will not be as obvious to consumers but are just as critical. 5G networks will increasingly rely on artificial intelligence, machine learning and intelligence at the edge to provide an optimal experience with available spectrum and infrastructure resources. When policymakers micromanage the network, they can short-circuit the innovations that ensure the network "just works." Plainly stated, communications networks work best when run by engineers, not lawyers.

It is important that the U.S. policymakers recognize that operators and infrastructure providers are a critical element of this virtuous cycle of innovation. Without the innovation in these market segments, innovation is more difficult in all of the others impeding the ability to meet consumer demands. Nokia therefore recommends that in evaluating regulations, the U.S. look to value creation in all areas of the mobile broadband ecosystem as a guiding principle and objective.

2. How can the U.S. Government best foster and promote the research, development, testing, and evaluation of new technologies and architectures; motivating domestic-based R&D (Questions 2-4)

Nokia recommends that the U.S. focus R&D incentives on three broad funding workstreams to ensure a thriving ecosystem for 5G and beyond. Although the focus in recent days among policymakers has been on providing R&D for open radio access networks ("ORAN"), doing so to the exclusion of 5G and 6G would be a critical mistake. Support in all three areas is essential.

Immediate funding to strengthen 5G capabilities: Around the globe, a common concern cited by governments and operators is that the R&D roadmap of the U.S. and its allies is not keeping pace with China's roadmap. While this concern is not valid across the board –

indeed there are many areas of the technology portfolio where trusted equipment suppliers are ahead of the Chinese in quality and capability -- there are nevertheless actions that the U.S. Government could take to further shore up R&D by trusted suppliers in the U.S.

Specifically, Nokia recommends a commitment of R&D funds administered through the National Institute for Science and Technology (NIST) or a similar agency to trusted suppliers to accelerate R&D roadmaps on critical 5G features, shorten any perceived gap in availability of functionality, and provide the U.S. with a comparative advantage in certain areas of technology. There are several areas where funding related to the 5G cycle could help bring capabilities of great interest to the market more quickly than current roadmaps forecast. For example, dynamic spectrum sharing and end-to-end secure network slicing are of great interest to commercial service providers and to federal users including the Department of Defense. A one-time commitment of $500 million or more could dramatically increase trusted supplier 5G capabilities providing new features, timely availability, and higher quality to U.S. carriers while bolstering the ability of trusted suppliers to secure deployments in other markets.

Early 6G Investment: While the focus of this NTIA request for comment is 5G, governments around the world already are funding 6G R&D with indications that the Chinese government has established at least two new government offices to coordinate 6G research and disseminate funds. As noted above, history indicates approximately a 10-year cycle between each generation of wireless. That 10-year cycle was accelerated for 5G and the U.S. should be prepared for similar acceleration moving forward. Based on that accelerated schedule, to keep pace, the U.S. should be prepared for the first 6G deployments before the end of the 2020s.

In order to ensure that the U.S. maintains its leadership position in wireless innovation, policymakers should create a multi-year funding program available to all trusted

suppliers and partners covering 6G foundational research into a range of wireless technologies including radio access networks, routing, and optical. Chief Technology Officers from across the 5G ecosystem are engaged in conversations now about a comprehensive 6G research agenda on which to cooperate. Nokia recommends further solicitation of comments laying out some of the broad areas of consensus for foundational 6G research and then providing, through the Department of Commerce, National Science Foundation or related agency, at minimum a sum of $500 million each year for three successive years, or $1.5 billion, to accelerate R&D in the critical early years of the development cycle for the next generation of mobile.

Focused U.S. investment in open networks: Network infrastructure is increasingly virtualized and cloud-based, lending unprecedented flexibility and agility to network architectures. There is also a movement to bolster the trusted supply chain through open radio access networks (ORAN). Nokia supports ORAN, and indeed was the first major equipment supplier to join the ORAN Alliance to work on technical specifications and, more recently, joined the ORAN Policy Coalition to advocate for support and funding to advance ORAN. Nokia recommends funding for open networks technology development as part of a smart, comprehensive approach to 5G and beyond technological leadership for the U.S. Specifically, policymakers should authorize funding through the Department of Commerce, National Science Foundation or related agency of $300-500 a year for three fiscal years to be administered for R&D and acceleration of commercial products for open networks.

Nokia believes that previous suggestions of a one-time funding allocation, for ORAN related R&D alone are flawed. Those proposals fail to provide enough funding, over a sustained period of time and cap the size of individual grants at a level that is unlikely to allow individual companies to conduct robust research. It is very likely that in addition to R&D

associated with the radio units (RU), baseband radios, and interfaces that connect them, there will be a need for substantial investment in new chip technologies and approaches. This will be expensive. A minimum of $1.5 billion will be needed over a period of years. The previous suggestions also fail to recognize that funding for 5G and even 6G research will have flow down benefits to the ORAN research agenda. Therefore, providing enough funding across the three recommended areas, and over several years, is a superior approach that not only ensures U.S. strength in 5G but in future Gs as well.

Strengthen Western Participation in Standardization: U.S. policymakers frequently raise concerns regarding the rapid increase in Chinese participation in global standards bodies accompanied by a stagnation or decline in U.S. participation. This has in turn raised concerns about substantial growth in IP generated within the standards by Chinese companies.

The U.S. has many potential participants in areas likely to be impacted by current and future wireless standardization, including automotive, healthcare, and utilities. Nokia sees two current barriers to increased participation by the U.S. and its trusted allies: (1) the cost of obtaining voting rights through accrediting bodies is prohibitive for many small and mid-sized companies and virtually all startups; and (2) the ongoing costs of contributing to standardization is extremely high. As such, Nokia recommends that the U.S. seek ways to reduce the costs of acquiring participation rights in key standards bodies as well as easing costs of sending experts to participate in working groups and of developing intellectual property to support the standards. Specifically, we recommend that the Administration direct the Internal Revenue Service to issue clarification that costs of participation in standardization are recognized for favorable treatment under the R&D tax credit and providing guidelines for the types of expenses that can be

recognized. Nokia also suggests that NIST explore ways to reduce the costs of obtaining voting memberships in key standards bodies through collaboration with the entities that provide such rights. It may also be appropriate to provide modest funding for grants to acquire voting memberships in standards bodies. A $5-10 million grant program would create a compelling opportunity to increase the participation of small and mid-sized U.S. companies, start-ups and vertical industries to obtain voting participation rights in standards bodies.

B. Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure

1. What factors should the U.S. Government consider in the development of core security principles for 5G infrastructure?

The major factors essential to the security of 5G are: trustworthiness of supplier and supply chain, flexibility of security approaches to allow customization and adaptability, unobtrusive operation, compliance and verification, and reliable people and processes. The infrastructure must ensure reliability, resiliency, and security if it is to promote trust. That will require trust in both the suppliers (their behavior, compliance, capability) and the supply chain (ability to deter, detect and mitigate risks to the equipment and software). A key way to match these factors to actionable policies is to consider them in the context of operational principles.

5G Security should be governed by principles that help us reach social and technological ambitions. The goal of these principles will be to assure public safety/national security, maintain uninterrupted functioning of critical infrastructure industries, promote network resiliency, and prevent and mitigate cyber-attacks by individuals and nation states.

First: Trust is essential as 5G enables automation and digitalization of many processes and services. The automation and digitalization of 5G use-cases need to be secure and reliable so that they are trustworthy and, as such, will be accepted by consumers and businesses.

5G strategy must contemplate current services (e.g. virtual workplace collaboration) as well as future services and applications (e.g., remote surgery assisted by Augmented/Virtual reality) that impact people and industries.

It is useful to distinguish between trust in supplier and trust in supply chain. They are not the same thing from either a policy perspective, with different approaches necessary to mitigate risks, or from an actual security perspective. For example, it is possible that a supplier has a track record of compliance with domestic laws, transparency of their operations and management decision-making, and no third-party relationships that cause concerns, yet there are nevertheless concerns about the security of their products because of poor quality or detection and mitigation practices. However, in such a case, policy makers can design policies to address supply chain hygiene concerns confident that defects in products are not maliciously intended.

If, however, policymakers do not have fundamental trust that the supplier is compliance oriented or if there are concerns that the supplier lacks transparency of ownership and management decision-making or may be influenced by third party actors then, regardless of the quality of the products and the security processes, mitigation of risk becomes more difficult. It may be necessary to create expensive monitoring and review programs, as indeed has been the case in several countries, that are time and resource intensive. Developing a framework of principles that define both trusted suppliers and trusted supply chains, and then holding suppliers to those principles, is a strong approach.

Second: Security must be customizable to address the vast number of use cases supported by 5G. 5G will allow interconnectedness of networks, devices and applications which need to handle many different privacy and security requirements at the same time. The interconnections enabled by 5G networks will have different classes of security risks and profiles

depending on the use and the sensitivity of the activity and associated data. Security should be designed so that the requirements for different users, services and industries can be orchestrated with robust performance levels and without impacting each other. Inflexible security, such as a "one approach fits all" model, would fail to account for unique threats and needs across the many sectors that will be served by 5G including military, public safety, health, utilities, and logistics among others. Fortunately, 5G will offer a robust range of options, including network slicing, wherein a user of a "slice" can customize the security approach to meet their needs and threat vectors.

Third: Security and privacy will be just as important in 5G's success as latency and reliability, and should operate in the background, imperceptible to the end-user. The complexity of underlying technology of 5G use cases, such as real-time remote healthcare and autonomous vehicles, should be transparent and seamless. Indeed, end-users should not routinely perceive the quality of their service – the service simply works. The user experience should be similar for 5G security, which will increase the trust and, thus, accelerate the growth in new 5G applications.

Fourth, critical infrastructure requires special attention, including a system for verification of compliance. Security for critical infrastructure requires a layered approach. As a first layer, we see 3GPP with its technical-specifications or -reports (e.g. TR33.501, TS33,210), which provides a good and proven foundation for government recommendations for options, features and capabilities. In specific critical infrastructure cases, enhancements to 3GPP may be warranted.

On top of 3GPP, multiple vendors have developed security safeguards or solutions, and this too is an area where the U.S. government could review and augment those

offered by vendors. Nokia's "NetGuard" security product, for example, goes beyond 3GPP standards for critical use cases and applies artificial intelligence, machine learning, and network level analytics to track malicious behavior and proactively implement corrective or protective actions.

Fifth, supply chain security is critical. Vendors must have internal controls ranging from the ethical behavior of employees to how products -- especially third-party components -- are reviewed to ensure no back doors or other high-risk implementations are allowed into the final product. Nokia secures its supply chain through a rigorous "Design for Security" governance model as well as proactive monitoring of live networks to better understand recent and imminent threats. Many of our commercial network customers employ third parties to do assessment of product risk. But many assessments are one-time manual exercises, which do not provide continuous security. Optimally, 5G qualified security configuration audits should be run by (semi-) automated products or tools very frequently from providers of 5G critical infrastructure.

2. What factors should the U.S. Government consider when evaluating the trustworthiness or potential security gaps in U.S. 5G infrastructure, including the 5G infrastructure supply chain? What are the gaps?

The U.S. Government should consider the use of widely accepted standards and certifications, such as those developed in 3GPP, in products/services. These standards and certifications should apply to the lead manufacturer and its supply chain. As discussed above, additional security can be layered onto this baseline level of security for critical infrastructure and other situations in need of heightened security.

Meeting basic security standards, and even heightened standards, however, can leave security gaps for reasons separate from the technology. For example, it is critical that 5G

networks rely on trusted suppliers and that the 5G networks are operated and maintained by trustworthy companies and individuals. To that end, Nokia recommends that the U.S. Government rely on set frameworks to evaluate supplier's strengths/weaknesses in the areas of business continuity, transparency of corporate governance and track record in delivering and maintain secure products.

3. What constitutes a useful and verifiable security control regime? What role should security requirements play, and what mechanisms can be used to ensure these security requirements are adopted?

5G networks cater to multiple types of industries and users, and not all have the same security requirements. Security controls for the healthcare sector will be different from those of utilities or finance, which in turn will different than less-sensitive consumer use cases.

There are general controls that are necessary for all industries, but not sufficient for all circumstances, including compliance with industry standards and best practices (e.g., 3GPP, IETF, NIST CSF, 800-53, GSMA NESAS, TL9000). Custom security controls, however, are required for specific use cases, such as those required to comply with NERC-CIP, HIPAA and the like. Non-technical controls are also critical, such as transparency of security/privacy practices, track record of trustworthiness, and a history of timely disclosure and remediation of security risks.

A verifiable security control regime consists of multiple layers, such as audits of vendor processes and the requirement for transparent reports on vulnerabilities uncovered during testing. There is no one-size-fits-all combination of controls appropriate to every situation. As a general matter, however, final product, system or software security testing prior commercial clearance would be beneficial (e.g. NIST CSF, GSMA, industry specific certifications). This should be very outcome oriented, specific, objective, actionable, and verifiable.

Nokia recommends that these requirements be organized into tiers which might be considered as representing levels of holistic 5G security and privacy achievement. Such measures could be complemented by live network real-time surveillance with proactive and automated shutdown, isolation capabilities. While proactive measures go a long way to ensuring that a system is secure, threats will happen (and frequently), requiring real-time monitoring and vigilance.

4. **Are there stakeholder-driven approaches that the U.S. Government should consider to promote adoption of policies, requirements, guidelines, and procurement strategies necessary to establish secure, effective, and reliable 5G infrastructure?**

U.S. service providers that operate 3G/4G networks have an excellent track record of maintaining secure networks. This is achieved through developing and implementing standards, best practices and policies. Public Private Partnerships (PPPs) between government stakeholders, operators and suppliers play a key role in developing standards and policies. U.S. CERT, NIST, CSRIC are good examples, where various stakeholders come together to promote network security. NIST CSF is a result of a successful PPP. These proven security verification models from PPPs should be evolved to build secure 5G networks. Active participation of U.S. stake holders in U.S. and global security standards organizations (ITU-T, ISO/IEC, ENISA) will also help in ensuring consistently high security standards across geographies creating a more secure global 5G network.

5. Is there a need for incentives to address security gaps in 5G infrastructure? If so, what types of incentives should the U.S. Government consider in addressing these gaps? Are there incentive models that have proven successful that could be applied to 5G infrastructure security?

5G Funding, Open Networks Funding, 6G Funding. Earlier in these Comments, we set forth potential funding mechanisms to bolster U.S. leadership in 5G, Open Networks and 6G. Security is essential to each of these technologies and basic funding to advance these technologies would almost certainly also advance their maturity with respect to security and trust. Of particular note are the potential security vulnerabilities in the early stages of open networks due to the integration of products supplied by multiple vendors. Open networks technologies must be shown to have security performance similar to classical RAN networks before they will achieve widespread adoption. Thus, it would be prudent that R&D funding for 5G, Open Network and 6G technologies include allocations of funds to advance the security component.

Incentives to extend the PPP standards-setting process to additional industries reliant on 5G. The current PPP model of developing resilient 3G/4G networks can be extended to 5G and outside of traditional telecom to reach connectivity of industries outside the traditional telecom realm. PPP models enable faster time-to-market and exchange of information. PPP models also result in developing common standards for a nation or region to implement new technologies in a fair and effective manner

For example, the U.S. Government can promote a PPP for health care, transportation etc. NCCoE CRADA is a good start, but it can be extended to cover more industries and the U.S. Government. This may be done through research grants, actively supporting global standards, promoting education and skills improvement for cybersecurity, providing incentives to adopt 5G adoption in various industries, etc.

Incentives to set up and retain initial security protocols for Federal systems and critical industry. Commercial networks have multiple security systems in place today. However, malicious intent is most likely dominated by individuals. Federal systems and critical infrastructure industries are far more likely to have malicious intent originate from state actors and organized criminals. For this reason, we should think of federal networks and 5G critical networks, as requiring a significant step up in security safeguards and internal controls to implement them. Therefore, incentive models for selected vendors should be considered so that true best in class products and networks can be produced. For example, imagine a vendor has been selected for radio access systems, and that federal systems requires hundreds of employee-*years* of R&D and testing labs to ensure all requirements are met, including clean rooms, if necessary. Such an investment may dampen interest in the project by otherwise qualified bidders. Some setup and retention incentive might prove useful in such a situation to encourage vendors to participate in federal systems in a trusted partnership.

Bug Bounty Program. A bug bounty program is an incentive already offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. These programs allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse. We suggest the U.S. government establish a 5G bug bounty program for 5G network function vulnerabilities based on peer reviewed reports of the 5G security vulnerabilities and solution approaches that are specific to 5G and not general in nature.

C. Line of Effort Four: Promote Responsible Global Development and Deployment of 5G

1. How can the U.S. Government best lead the responsible international development and deployment of 5G technology and promote the availability of secure and reliable equipment and services in the market?

Nokia recommends that the U.S. continue to lead by example in demonstrating to other nations the importance of secure and trusted infrastructure through the articulation and adoption of principles and practices that define both trusted suppliers and trusted supply chains. Noting the manner in which 5G will become a ubiquitous technology underpinning not just conventional wireless communications, but also connectivity for enterprises, automated factories, utilities, transportation and health care delivery among others, the need to ensure resilient, reliable, and secure infrastructure within the 5G network is of heightened importance.

Prior to allowing a supplier of 5G network equipment or software to deploy a solution, policymakers in all governments should insist, at a minimum on the following:

- Transparency in ownership and management of a supplier. This includes determining whether individuals or states with a history of cyber espionage, IP theft, data mining or other nefarious practices are part of the ownership or management decision making of a supplier;
- The establishment and adherence to important norms of corporate conduct including robust compliance programs, due diligence and human rights programs, and a history of complying with the domestic laws of the countries in which they seek to operate;
- Well-developed supply chain programs that both focus on security from the design and product development stage through deployment and the lifecycle of the equipment.

Companies that can demonstrate these attributes are likely trustworthy partners and providers of trustable solutions. When using such suppliers, a government can have confidence that when defects are discovered in a product they are not there purposefully, but rather are the result of error or failure to anticipate a vulnerability, and confidence will be high that the vulnerabilities will be remediated quickly and cooperatively. Suppliers that cannot demonstrate these attributes would require, if permitted, substantially greater resources to monitor and mitigate risk.

Indeed, this is the approach the U.S. has taken with respect to its own domestic 5G deployments and that it has recommended to other nations. But simply modeling this trust-based approach may not be sufficient to encourage the development of a global system of interconnected networks that is safe, secure and sustainable. As noted below, the U.S. may need to provide support to other nations to encourage adoption of trustworthy suppliers, effectively ensuring that decisions are made from a technical, security, and performance perspective, and not simply on the basis of financing terms.

2. How can the U.S. Government best encourage and support U.S. private sector participation in standards development for 5G technologies?

There is no doubt that participation from a variety of industries and countries will benefit standards bodies. These bodies function well precisely because they are democratically oriented and focus on consensus among experts on the best engineering and science behind approaches that are recommended and adopted. We should not turn these bodies into battlefronts in escalating tensions between nation states. Politicization of standards bodies will actually undermine them as viable, attractive places for scientific discourse leading to high quality standards that drive scale in global development and manufacturing.

Nokia suggests a focus on understanding the potential causes of muted participation from certain countries and certain sectors. One fairly obvious topic from our

perspective is both the cost of obtaining the requisite voting memberships in standards bodies like 3GPP and the cost to companies of contributing staff time and technology to the development of standards. Although Nokia is a large company with a long heritage in standards bodies, even our participation levels are from time to time impacted by the business cycle. Therefore, it is quite reasonable to assume that smaller companies with more limited resources find the cost of maintaining headcount for the purposes of travelling to standards meetings and contributing the time and their technology to be almost prohibitive.

Similarly, vertical industries previously less impacted by developments in wireless standards, for example, may not have found engagement in standards bodies to be an edifying or value enhancing proposition. However, with the huge technical advances in 5G, reliance on wireless technology will reach historic levels and the outcome of standardization work on issues like encryption, spectrum slicing, and multi-level authentication among others will be of much greater interest to end user industry segments like auto OEMs and utilities. It is therefore essential to encourage their participation through outreach and through incentives.

As discussed above, Nokia recommends two possible approaches to address the cost of participation in standardization. First, with respect to obtaining voting memberships Congress could appropriate a sum of money, likely in the millions of dollars, to NIST to award grants to qualifying small entities to offset the cost of obtaining such memberships.

Second, policymakers could encourage the IRS to clarify that certain costs associated with participation in standardization are deductible under the permanent R&D tax credit. Nokia does not believe this would require a change in the R&D tax credit authorizing legislation, but rather a clarification from the IRS following a Notice of Inquiry/Request for Comment through which it could solicit comments on the appropriate types of expenses which

might be recognized (i.e., portions of an employee's salary attributable to their work on behalf of the company in standards working groups, travel costs to plenary meetings, and other reasonable expenses). For larger companies, modest tax assistance could allow for the further increase in participation levels. For small companies, such assistance may be essential to the threshold decision to participate at all.

3. Are there market or other incentives the U.S. Government should promote or foster to encourage international cooperation around secure and trusted 5G infrastructure deployment? (Question 4)

As previously noted, the decision on suppliers may be very dependent on the financial health of the operator and whether its financial circumstances allow for the selection of vendors with the highest performing technology, greatest reliability and security, or lead it to devalue those factors in favor of the least expensive technology. If the U.S. expects other nations to demonstrate the same level of commitment to resilience, reliability, and security even though such qualities may add cost, the U.S. may need to bring resources forward to assist these countries and operators.

As an example, an operator might very much like to switch a supplier or introduce an additional supplier to their vendor domain. However, their existing supplier may have advantages in localized personnel over a potential new supplier that may need to invest heavily to create a similar level of personnel support, the removal of equipment and replacement with a new supplier might require expertise beyond the capability of a nation or operator (engineering and planning) or one supplier might have access to financing support unavailable to the commercial market writ large that confer an advantage

In circumstances such as those outlined above, the U.S. can provide financial support to developing nations through any number of entities such as the State Department or US

AID so that government officials and operators can develop the skills to take on the challenges of managing a highly competitive, multi-vendor ecosystem. In addition, the Development Finance Corporation (DFC) and the U.S. Export Import Bank (ExIm) can become more engaged in telecommunications infrastructure projects to ensure the availability of financing that allows nations and operators the chance to choose form a variety of suppliers with similar financing terms rather than the current environment where some suppliers are squeezed out of a procurement by financing support for one supplier that is not broadly available from commercial banks to allow a real choice.

In a circumstance where nations and operators have the ability to choose from a range of suppliers offering technology solutions and financing packages that are compelling, they can choose to prioritize the selection of suppliers that meet the profile they seek in a partner in terms of reliability and security. In developing markets this remains elusive. Despite the expression of support for expanding the availability of financing from US ExIm and DFC, the progress has been modest. In the case of ExIm, there is a need to modernize several of its policies to match the practices of other global export credit agencies (ECAs) including the content policy that drives the level of financing available for a project. Other ECAs have liberalized their policies to include, for example, the attribution of related R&D and manufacturing done by domestic companies regardless of location (i.e., a U.S. company manufacturing an item in another country would be attributable under most ECAs' rules by virtue of being a U.S. company). U.S. ExIm has shown reluctance to modernize its policies.

Effectively this means only a limited number of deals might qualify, or qualify at levels that make the deals comparable to what is offered with support from an entity like the Chinese Development Bank. If the U.S. is serious about providing financial tools that can realistically give developing countries and their operators more choices, modification of some of the existing rules and policies needs to be addressed even if only for 5G projects as an exception.

Respectfully submitted,

Nokia

/Brian Hendricks/
Brian Hendricks
Jeffrey Marks
Government Relations

Nokia
601 Pennsylvania Avenue, NW
South Building, Suite 900
Washington, DC 20004

June 25, 2020