June 25, 2020

Mr. Travis Hall
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, District of Columbia 20230

RE: The National Strategy to Secure 5G Implementation Plan (Docket No. 200521-0144 and RIN 0660-XC04)

ACT | The App Association (App Association) appreciates the opportunity to submit the following comments to the United States Department of Commerce's National Telecommunications and Information Administration (NTIA) to inform the development of an Implementation Plan for the National Strategy to Secure 5G,[1] pursuant to the Secure 5G and Beyond Act of 2020.[2]

The App Association represents approximately 5,000 small- to medium-sized software application developers and connected device companies across the globe. Our members leverage the connectivity of smart devices to produce groundbreaking software solutions that impact Americans' everyday lives. We are committed to American leadership in 5G, as well as supporting a regulatory environment that promotes the deployment of 5G infrastructure.

The App Association's members are at the forefront of the mobile revolution in both rural and urban areas, innovating across a variety of sectors including healthcare, agriculture, finance, and entertainment, providing the touchpoint for the internet of things (IoT) across consumer and enterprise use cases. App Association member companies lead the $1.7 trillion app economy in the U.S. and employ 5.9 million Americans. The App Association's members rely on far-reaching and fast mobile internet connections to meet market needs and to develop the internet of things (IoT) across consumer and enterprise use cases. They have a large stake in the ability of the US to host and drive the development of 5G networks and the innovation that occurs on top of 5G standards.

---

[1] *The National Strategy to Secure 5G Implementation Plan*, 85 FR 32016 (May 28, 2020).

[2] Secure 5G and Beyond Act of 2020, Public Law No. 116-129, 134 Stat. 223-227 (2020).

The future of the app economy depends on the strength and density of America's wireless and wired backhaul networks. Economic analysis conducted by the App Association shows that deployment of 5G wireless networks will create 8.5 million jobs in the U.S. over the next five years, enabling improvements in economic productivity, employment, and consumer value.[3] 5G will affect the labor market through direct and indirect means; while the additional labor required to build out the network to deploy 5G will certainly create the most immediate demand for new jobs, the broadest impact on the labor market comes from new employment opportunities through the way 5G will enable new applications, services, ways of doing business, and general growth of businesses. Workers benefitting from this deployment will earn more than $560 billion during that time, create $1.7 trillion in additional output, and add over$900 billion to U.S.GDP.

Recent 5G pilots have demonstrated the technology's ability to provide staggering internet speeds, more than 75 times the speed of 4G LTE. While 4G LTE helped make the internet more accessible on mobile devices, 5G offers ultra-low latency to its users, giving mobile infrastructure the reliability needed for the applications that depend on network integrity. These enhancements can provide a highly tailored service to meet specific customer needs. More specifically, it enables our members to make data-rich applications that require high-quality connections that allow faster data transfer and information sharing between workers who may be at a virtual desk, at a medical clinic, in an IoT-enabled warehouse, or with a customer in the store.

The potential of the 5G revolution and expanded use of unlicensed spectrum is more significant than merely providing access. It will also increase internet speeds, add bandwidth, and lower latency in a way that benefits business-to-business interactions and IoT-driven machine-to-machine communications. Once we make this connection, we can bring the app economy to the next level.

The App Association therefore supports the federal government's development of an Implementation Plan for the National Strategy to Secure 5G. Further, we offer the following specific inputs on various questions posed on the Strategy's line of efforts:

Spectrum: The future of IoT innovations and the app economy will depend on the strength and density of 5G networks, which are supported by myriad spectrum bands and different types of infrastructure, including small cell deployment, that seamlessly work together. Failure to adequately develop US infrastructure and finite spectrum resources will harm both the economy and consumers. The prospect of countless connected devices entering our communications networks through nodes in homes,

[3] James Prieger, "An Economic Analysis of 5G Wireless Deployment: Impact on U.S. and Local Economies" (Feb. 2020), *available at* https://ecfsapi.fcc.gov/file/10417521421416/ACT%20Ex%20Parte%20Notice%20re%205G%20Economic%20Analysis%202020.pdf.

workplaces, or other last-mile connectivity endpoints will dramatically increase data flows across communications networks. Macro sites alone will not be sufficient to manage the congestion, making realization of a robust 5G network critical for the U.S. The Strategy should set the identification of new opportunities for reallocation and/or new sharing arrangements across spectrum bands consistent with interference protection principles, including for government-owned spectrum bands that may be ideal for commercial IoT use, particularly mid-band and millimeter wave bands.

Infrastructure Deployment: The App Association urges the Strategy to prioritize an improved and streamlined process for approval and siting of 5G equipment in the U.S. Differences in local zoning, siting, and approval processes across localities have made the deployment of infrastructure difficult, too expensive, and inefficient. The App Association supports recent steps by the Federal Communications Commission to speed upgrades to existing towers (adding, removing, and switching out equipment).[4] The Strategy should provider for coordinated federal efforts to enable 5G infrastructure deployment in and on both federal facilities and commercial buildings.[5]

Cybersecurity: While 5G will enable the rise of IoT applications with many benefits, it also raises security threats. Due to a broadened attack surfaces, the rise of IoT will require more evolved and dynamic risk management practices. No data is more important to Americans than their own personal information. Our members appreciate the personal value of our data and put extensive resources into ensuring the security and privacy of end user data. These practices help earn and maintain consumer trust and meet market demand.

We support ongoing and emerging public-private partnership initiatives and strategies to improve the nation's cybersecurity risk management efforts, and we continue to work with our members to advance improved cybersecurity risk management practices. Small businesses represent 99.7 percent of all U.S. firms,[6] and they require heightened assistance. It is important that policymakers remain mindful of the fact that large companies often dedicate large budgets to create and maintain cybersecurity control processes and have the ability to hire staff and consultants to mitigate cybersecurity risks. Unfortunately, small- and medium-sized enterprises (SMEs) do not. For many of our members, the role of chief security officer may be one of five hats worn by a single employee. The essential role of American small businesses, along with the unique resource constraints they face, make the Strategy and any efforts made pursuant to it even more important to the security and stability of the nation's critical infrastructure. The App Association notes its continued support of the NIST Cybersecurity Framework which provides a scalable, flexible, voluntary toolbox that any organization can use to reduce vulnerabilities, prevent intrusions, and mitigate damage caused by cybersecurity

[4] https://www.fcc.gov/document/fcc-acts-accelerate-deployment-5g-wireless-infrastructure-0.

[5] E.g., https://www.fcc.gov/document/orielly-letter-secretary-dan-brouillette-department-energy.

[6] https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf.

attacks.

Further, we note that app economy innovators across the U.S. depend on leading technical data protection methods, such as the use of strong encryption techniques, to keep users safe from harms such as identity theft. However, interests within the U.S. government and abroad continue to demand that "back doors" be built into encryption for the purposes of government access. These policies would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. The viability of a small app development company's product from a security and privacy standpoint depends on the trust of its end users. We strongly recommend that the Strategy support the use of strong encryption techniques to enable 5G cybersecurity.

Standards and Access to Standardized 5G Technologies: NTIA appropriately requests information on how the U.S. Government can best encourage and support U.S. private sector participation in standards development for 5G technologies. The App Association strongly encourages the Strategy to support public-private collaboration on 5G through standardization by encouraging key U.S.-based standard-setting organizations (SSOs) to grow and thrive. The U.S. government can support such organizations through pro-innovation policies that encourage private sector research and development of 5G innovations and the development of related standards, consistent with OMB Circular A-119.[7]

It is critical that the Strategy provide that such 5G standards are accessible to innovators through promoting openness, consensus-based decision making, transparency, and inclusivity. A cornerstone to ensuring this accessibility must be through promoting a balanced approach to standard-essential patent (SEP) licensing.[8] 5G technical standards, built on contributions through an open and consensus-based process, bring immense value to consumers by promoting interoperability while enabling healthy competition between innovators; and often include patented technology. Offering patented technology to a standard can represent a clear path to reward in the form of royalties from a market that likely would not have existed without the wide adoption of the standard. To balance this potential with the need for access to the patents that underlie the standard, many standards setting organizations (SSOs) require holders of patents on standardized technologies to license their patents on fair, reasonable, and non-discriminatory (FRAND) terms. FRAND commitments prevent the owners of patents used to implement the standard from exploiting the unearned market power that they otherwise would gain as a consequence of the broad adoption of a standard. Once patented technologies incorporate into standards, it compels

[7] Revision of OMB Circular No. A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities", 81 FR 4673 (Jan. 27, 2016).

[8] Notably, OMB Circular A-119 defines a "voluntary consensus standard" to include those that "requir[e] that owners of relevant intellectual property have agreed to make that intellectual property available on a non-discriminatory, royalty-free or reasonable royalty basis to all interested parties." *Id*.

manufacturers to use them to maintain product compatibility. In exchange for making a voluntary FRAND commitment with an SSO, SEP holders gain the ability to obtain reasonable royalties from a large number of standard implementers that might not have existed absent the standard. Without the constraint of a FRAND commitment, SEP holders would have the same power as a monopolist that faces no competition.

Unfortunately, a number of owners of FRAND-committed SEPs are flagrantly abusing their unique position by reneging on those promises with unfair, unreasonable, or discriminatory licensing practices. These practices, under close examination by antitrust and other regulators in many jurisdictions, not only threaten healthy competition and unbalance the standards system but also impact the viability of new markets such as 5G. This amplifies the negative impacts on small businesses because they can neither afford years of litigation to fight for reasonable royalties nor risk facing an injunction if they refuse a license that is not FRAND compliant. The App Association shares the view of the courts that the entrenchment of monopoly power, and the market distortions that SEP abuse engenders, threaten to irreparably harm the marketplace at this critical stage of 5G deployment.[9]

Patent policies developed by SSOs today will directly impact the way we work, live, and play for decades to come. SSOs vary widely in terms of their memberships, the industries and products they cover, and the procedures for establishing standards. Each SSO will need the ability to tailor its intellectual property policy for its particular requirements and the needs of its membership. The App Association believes that some variation in patent policies among SSOs is necessary and that the U.S. government should not prescribe detailed requirements that all SSOs must implement, which should be reflected in the Strategy. At the same time, however, as evidenced by the judicial cases and regulatory guidance, basic principles underlie the FRAND commitment and serve to ensure that standard setting is pro-competitive, and the terms of SEP licenses are in fact reasonable. Ideally, an SSO's intellectual property rights policy that requires SEP owners to make a FRAND commitment would include all of the following principles that prevent patent "hold up" and anti-competitive conduct:

- **Fair and Reasonable to All** – A holder of a SEP subject to a FRAND commitment must offer to license such SEP on fair, reasonable, and nondiscriminatory terms to all companies, organizations, and individuals who implement or wish to implement the standard.
- **Injunctions Available Only in Limited Circumstances** –SEP holders should not seek injunctions and other exclusionary remedies nor allowed these remedies except in limited circumstances. The implementer or licensee is always entitled to assert claims and defenses.
- **FRAND Promise Extends if Transferred** – If there is a transfer of a FRAND-encumbered SEP, the FRAND commitments follow the SEP in that and all subsequent transfers.

[9] *E.g.*, *FTC v. Qualcomm Inc.*, Case No. 5:17-cv-00220 (N.D. Cal. May 21, 2019).

- **No Forced Licensing** – Patent holders should not require implementers to take or grant licenses to a FRAND-encumbered SEP that is invalid, unenforceable, or not infringed, or a patent that is not essential to the standard.
- **FRAND Royalties** – A reasonable rate for a valid, infringed, and enforceable FRAND-encumbered SEP should be based on several factors, including the value of the actual patented invention apart from its inclusion in the standard, and cannot be assessed in a vacuum that ignores the portion in which the SEP is substantially practiced or royalty rates from other SEPs required to implement the standard.

We also note that a number of SSO intellectual property rights policies require SSO participants to disclose patents or patent applications that are or may be essential to a standard under development. Reasonable disclosure policies can help SSO participants evaluate whether technologies considered for standardization are covered by patents. Disclosure policies should not, however, require participants to search their patent portfolios as such requirements can be overly burdensome and expensive, effectively deterring participation in an SSO. In addition, FRAND policies that do not necessarily require disclosure, but specify requirements for licensing commitments for contributed technology, can accomplish many, if not all, of the purposes of disclosure requirements. Key U.S. antitrust agencies such as the Federal Trade Commission, have provided long-standing backing to the need for a balanced approach to standardization and patents, which the Strategy should leverage. The Strategy must support American SSOs in this respect, and enable their governance of their own processes consistent with the above.

The App Association also notes its strong opposition to recent steps taken by the Department of Justice to eliminate the role of competition law in SEP disputes (in contradiction to federal law and court precedent), and to legitimize false narratives claiming that U.S. competitiveness and national security will be harmed unless select U.S. companies are allowed abuse their voluntary FRAND commitment. These steps taken by DOJ have damaged the U.S.' ability to globally lead in pro-innovation policy and law and have no place in the Strategy. Abandonment of well-established SEP law and policy jeopardizes the open standardization process that should be a cornerstone of a successful 5G strategy for the U.S. and enables abuse in standards and in SEP licensing scenarios by foreign competitors.

The App Association appreciates the opportunity to provide its recommendations on the development of an Implementation Plan for the National Strategy to Secure 5G.

Respectfully submitted,

Brian Scarpelli
Senior Global Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
202-331-2130