Before the
U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, D.C.

The National Strategy to Secure 5G Implementation Plan	)))))	Docket No. 200521–0144 RIN 0660-XC047

COMMENTS OF NCTA -
THE INTERNET AND TELEVISION ASSOCIATION

NCTA – The Internet & Television Association (NCTA)[1/] hereby submits its comments in response to the Request for Comments (RFC) issued by the National Telecommunications and Information Administration (NTIA) in the Department of Commerce (Department) to help inform the development of an Implementation Plan for the National Strategy to Secure 5G.[2/] The RFC was prompted by the enactment earlier this year of the Secure 5G and Beyond Act of 2020,[3/] which requires the development of a strategy to ensure the security of next-generation wireless communications systems and infrastructure.

INTRODUCTION AND SUMMARY

NCTA supports the objective of preserving and strengthening U.S. leadership in the development and secure deployment and operation of 5G and other advanced wireless

---

1/ NCTA is the principal trade association of the cable television industry in the United States, which is a leading provider of residential broadband service to U.S. households. Its members include owners and operators of cable television systems serving nearly 80 percent of the nation's cable television customers, as well as more than 200 cable program networks. Cable service providers have invested more than $290 billion over the last two decades to deploy and continually upgrade networks and other infrastructure—including building some of the nation's largest Wi-Fi networks.

2/ Department of Commerce, National Telecommunications and Information Administration, *The National Strategy to Secure 5G Implementation Plan*, Docket No. 200521–0144, 85 Fed. Reg. 32016 (May 28, 2020) ("RFC").

3/ Secure 5G and Beyond Act of 2020, Public Law No. 116–129, 134 Stat. 223–227 (2020) ("Act").

communications systems and infrastructure. Its member companies play a key role in the broader 5G infrastructure and ecosystem. For example, cable companies will provide wireline backhaul to networks for 5G traffic and services and will offer 5G services as Mobile Virtual Network Operators (MVNOs). Importantly, 5G is not the only advanced wireless communications technology available to Americans. Next-generation Wi-Fi is already offered using existing unlicensed spectrum bands and will be boosted by the Federal Communications Commission's (FCC) recent decision to make spectrum in the 6 GHz band available for unlicensed use. Wi-Fi carries over half of U.S. internet traffic, and now more than ever before Americans are using Wi-Fi to work and learn from home, shop for essentials, and connect with doctors and loved ones. Moreover, Wi-Fi will be an important part of the 5G ecosystem, with one estimate projecting that over 70% of 5G traffic will be offloaded to a Wi-Fi network by 2022.[4/] Federal policy should support and promote the considerable innovation taking place not just in 5G wireless networks, but also in wireline and Wi-Fi networks that are involved in transmitting the vast majority of wireless voice and data transmissions.

The breadth of the ecosystem undergirding 5G and other next-generation wireless communications systems and infrastructure – encompassing spectrum, small cell antenna equipment, poles, towers and other siting facilities, core radio networks, backhaul facilities, wireline networks, and Wi-Fi networking equipment – underscores the importance of crafting an implementation plan that is technology- and business model-neutral and based upon voluntary best practices developed through multi-stakeholder practices. The Administration's policies should promote security and innovation at all layers of this ecosystem, by drawing upon the success of security initiatives and frameworks emerging from a variety of ongoing multi-

[4/] *See infra* at text accompanying n. 13.

stakeholder, public-private partnerships. The plan emerging from this proceeding also should promote competition and vendor diversity and encourage U.S. global leadership in standards and specifications work, including work based upon open security principles.

The Administration should ensure that rules under consideration in other proceedings do not inadvertently or unnecessarily hamper research and development (R&D), technical specification and standards work, and product testing required to preserve U.S. technology leadership in advanced communications systems and infrastructure. In conjunction with its rulemaking to implement the directives in Executive Order 13873 regarding supply chain risks arising from information and communications technology and services (ICTS), the Department should ensure that constraints on ICTS transactions do not encompass R&D, standards-setting and specifications work, and product testing activities and agreements.

The Department recently amended its rules to clarify that participating in certain standards-setting activities with Huawei, notwithstanding its inclusion on the prohibited Entity List, would not trigger a license requirement or other constraints associated with interacting with a company on the Entity List.[5/] This decision is a step in the right direction that wisely recognizes the importance of preserving and strengthening U.S. global leadership by ensuring that American companies may freely participate in world-wide standards-setting activities. The Department should ensure that its policies developed in this and related proceedings likewise promote – and do not hinder – substantial involvement by U.S. companies in setting the standards and specifications that will be used to effectuate security worldwide for 5G and other advanced wireless communications systems and infrastructure.

[5/] Press Release, *Commerce Clears Way for U.S. Companies to More Fully Engage in Tech Standards-Development Bodies,* Department of Commerce (June 15, 2020), https://www.commerce.gov/news/press-releases/2020/06/commerce-clears-way-us-companies-more-fully-engage-tech-standards.

I. ANY 5G STRATEGY SHOULD BE TECHNOLOGY-NEUTRAL AND PROMOTE DEPLOYMENT OF ALL ELEMENTS OF NEXT-GENERATION WIRELINE AND WIRELESS COMMUNICATIONS SYSTEMS AND INFRASTRUCTURE

The cable industry is a key part of the 5G ecosystem and a significant provider of next-generation wireline and wireless communications systems and infrastructure. Cable operators play an important role in supporting the widespread deployment and growth of 5G networks. 5G and other advanced wireless systems and infrastructure will combine computing, communications, and cloud-based capabilities to enhance mobile broadband, unleash new Internet of Things (IoT) features and services, and provide users with faster speeds and ultra-low latency. Cable's wireline network infrastructure will help meet critical backhaul needs for 5G networks.[6/] Many of NCTA's members have deployed hybrid fiber-coaxial networks capable of gigabit-per-second speeds throughout their footprints. And as cable moves toward providing 10G—services capable of 10 gigabit per second speeds—over the next few years, NCTA members' networks will be even more robust in their capability to support the end-to-end speed and latency needs of 5G small cells, which will rely on wireline networks. Federal policies designed to foster security and investment for advanced wireless infrastructure may not be fully effective unless they also promote deployment of the wired backhaul necessary to support 5G small cell networks. NCTA's members are also offering 5G services themselves as MVNOs and have expressed interest in deploying in new 5G-suitable spectrum bands, such as 3.5 GHz.

Cable operators are also providers of advanced Wi-Fi networks that will benefit all Americans by serving as both a supplement and in some cases an alternative to 5G network

---

6/ *See, e.g.,* E. Gronvall, *Cable's Role in the 5G Evolution*, COMMSCOPE, (2018), https://www.nctatechnicalpapers.com/Paper/2018/2018-cable-s-role-in-the-5g-evolution; CableLabs, *Cable: 5G Wireless Enabler,* at 4 (Winter 2017), http://www.cablelabs.com/wp-content/uploads/2017/02/cable-5g-wireless-enabler.pdf ("Cable operators have deployed vast broadband networks across the globe. Since wireless services rely on fixed network connectivity, this positions cable to be a key enabler of 5G.").

capacity and capabilities.[7/] American businesses already depend on Wi-Fi to deliver important services to American consumers, including not only wireless broadband, but also healthcare monitoring and connected medical devices, factory automation, asset tracking, smart farming solutions, and home security monitoring. Wi-Fi already carries over half of all internet traffic in the United States, and that trend is expected to continue to grow.[8/] The annual economic contribution of unlicensed technologies such as Wi-Fi to the United States economy is substantial —approximately $499 billion in 2018 alone, and projected to nearly double to $993 billion annually by 2023.[9/]

The FCC's recent decision to open additional mid-band spectrum for unlicensed use in the 6 GHz band provides a tremendous opportunity to enhance the features and capabilities of advanced Wi-Fi offerings.[10/] The latest generation of Wi-Fi technology, Wi-Fi 6, offers multi-gigabit speeds, lower latency, greater throughput, and can support more devices on the network[11/] – which will support the anticipated proliferation of IoT devices, artificial intelligence offerings, and machine-to-machine communications. The roll-out of the next generation of unlicensed technologies in the 6 GHz band will support wide-bandwidth Wi-Fi, as well as

---

7/ *See. e.g., Cisco Annual Internet Report (2018-2023)*, at 14, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf (*Cisco Annual Report)* ("Wi-Fi has a powerful role to play alongside other small cell technologies in delivering key use cases going forward in the 5G Era").

8/ VNI Complete Forecast Highlights, United States, https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/United_States_2022_Forecast_Highlights.pdf. *See also infra* at n. 13.

9/ Raul Katz & Fernando Callorda, Telecom Advisory Services, LLC, *The Economic Value of Wi-Fi: A Global View (2018 and 2023)* at 6-7, 33-34 (2018), https://morningconsult.com/wpcontent/uploads/2018/10/Economic_Value_of_Wi-Fi_2018.pdf.

10/ *In the Matter of Unlicensed Use of the 6 GHz Band*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3852 (2020).

11/ Cisco's Annual Internet Report predicts that in North America, the number of networked devices will increase from 3 billion in 2018 to 5 billion by 2023. *Cisco Annual Report* at 4. Approximately 75 percent of those networked devices—3.4 billion—will either be wired or "connected over Wi-Fi." *Id.*

innovative, data-intensive applications like connected healthcare, immersive training and educational opportunities, as well as high-resolution virtual and augmented reality applications.

Demands on Wi-Fi capacity will become even more acute as the United States continues to progress into a 5G world. The 5G future will generate vast amounts of new data traffic and will rely on a combination of licensed, unlicensed, and coordinated shared spectrum frequencies to deliver on 5G's promises of higher speeds and lower latencies. And while unlicensed spectrum will continue to carry the majority of traffic in the 5G environment, even cellular 5G will rely on unlicensed technologies like Wi-Fi to offload large amounts of data: "[t]he paradox of [licensed] 5G is that although it provides more bandwidth" compared to previous generations, "it will also support so much more data usage that even more offload is required," including to "unlicensed Wi-Fi technology."[12/] Indeed, over 70% of 5G data traffic is expected to be offloaded to Wi-Fi by 2022.[13/]

In addition, Wi-Fi will bring multi-gigabit speeds and higher-capacity connections to areas where cellular 5G will not reach in the near future, such as in rural and remote areas, and to indoor areas where cellular signals may be weak. Thus, expanding the footprint of 5G and next-generation wireless offerings throughout the United States in urban, suburban, and rural environments, will require both licensed and unlicensed spectrum. In short, both wireline and Wi-Fi networks are indispensable technologies for ensuring wireless connectivity for all Americans and promoting the growth of 5G networks. The national strategy for 5G should

---

12/ Wireless Infrastructure Association, *The 5G Paradox: The Need for More Offloading Options in the Next-Generation Wireless Era* 2 (Feb. 8, 2019), https://wia.org/resource-library/the-5g-paradox-the-need-for-more-offloading-options-in-the-next-generation-wireless-era/.

13/ Broadcom, *Wi-Fi in the 5G Era,* at slide 24 (2019), https://newamericadotorg.s3.amazonaws.com/documents/Wi-Fi_in_the_5G_Era_-_Broadcom_presentation.pdf.

support and implement policies that promote growth and innovation in all segments of the 5G ecosystem.[14/]

II. THE SECURE 5G STRATEGY SHOULD BUILD UPON AND REINFORCE VOLUNTARY APPROACHES TO NETWORK SECURITY UNDERWAY IN VARIOUS MULTI-STAKEHOLDER PROCESSES

The government's ongoing efforts to streamline deployment policies for wireless and wireline networks and to make more licensed and unlicensed spectrum available to support next-generation technologies will enable wireline networks, Wi-Fi, and 5G to work together to deliver high throughput connectivity across the country. But that objective requires a policy framework that is both technology- and business model-neutral, to ensure that American consumers continue to have access to the most advanced and innovative wireless technology offerings. The Federal government should refrain from policies and decisions that distort the free market or give preferences to one wireless technology over another, or to wireless technologies over wireline. In an environment where wireline and wireless technologies converge and become ever more interdependent, the Department should strive to adopt policies that promote growth, investment, interoperability, and security for all types of companies using all types of technologies.

A broad array of new services, features, and capabilities is emerging across the wireless ecosystem. Innovation is occurring in the 5G radio access networks (RANs), the 5G core, backhaul technologies that support connecting 5G RANs to wireline networks, the core wireline network itself, and in next-generation wireless offerings and capabilities such as Wi-Fi that rely on unlicensed bands. Companies involved in developing and providing next-generation wireless

---

[14/] *See In the Matter of Accelerating Wireline Broadband Infrastructure Development by Removing Barriers to Infrastructure Investment; Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment*, WC Docket No. 17-84, WT Docket No. 17-79, Comments of NCTA (June 15, 2017).

systems and infrastructure have strong incentives to address security issues to encourage adoption and use of 5G devices and offerings, along with other advanced wireless services.

Developing and implementing a secure 5G strategy warrants a "whole of government" response, involving not only NTIA and the Department, but coordination with other agencies and public-private partnerships involved in addressing the wide range of security issues implicated here. Efforts to secure 5G should build upon – and need not differ from – voluntary, consensus-driven approaches and initiatives underway across the technology landscape. The NIST Cybersecurity Framework provides guidelines for network providers and all other entities involved in deployment and operation of advanced wireless and wireline network systems and infrastructure.[15/] NIST's special publication designed to assist federal agencies, companies, and other organizations in managing cybersecurity and privacy risks when deploying and using IoT devices also offers helpful guidance for strengthening 5G network and product security.[16/]

There is ongoing activity in a wide variety of industry bodies and working groups that is directly relevant and responsive to 5G security issues. This includes work by 3GPP[17/], Telecom Infra Project (TIP)[18/], the Global System for Mobile Communications Association (GSMA),[19/] the Internet Engineering Task Force (IETF),[20/] the Messaging, Malware, and Mobile Anti-Abuse

---

15/ *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute of Standards and Technology, (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

16/ *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NISTIR 8228, (June 2019), https://csrc.nist.gov/publications/detail/nistir/8228/final.

17/ *See* https://www.3gpp.org/news-events/1975-sec_5g.

18/ *See* https://telecominfraproject.com/who-we-are/

19/ *See e.g., Securing the 5G Era*, https://www.gsma.com/security/securing-the-5g-era/.

20/ *See e.g., 5G Security Standards: What are They?* (June 10, 2020), https://www.sdxcentral.com/5g/definitions/5g-security-standards/ (Noting collaboration between 3GPP and IETF on development of 5G security standards); *Security architecture and procedures for 5G system*, v. 16.2 (March 27, 2020), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.

Working Group (M3AAWG),[21/] the FCC's Communications Security, Reliability and Interoperability Advisory Council (CSRIC),[22/] and ongoing efforts under the Department's own Botnet Roadmap.[23/] There is also important work related to 5G security taking place at the Department of Homeland Security (DHS) in conjunction with the activities of the ICT Supply Chain Risk Management Task Force.[24/] The task force, a public-private partnership, is co-chaired by the Communications and the IT Sector Coordinating Councils (CSCC and IT-SCC). It has a two-year charter to identify and manage risk to the global ICT supply chain, with a specific focus on bolstering supply chain security for 5G and other next-generation networks.

Most of the ongoing initiatives noted above operate as multi-stakeholder groups or public-private partnerships. The success of these efforts reflects the efficacy of their foundational principles: (i) collaboration with industry, (ii) consensus-driven best practices, (iii) flexible standards, and (iv) voluntary adoption and usage. The Department's efforts on 5G should follow the multi-stakeholder and public-private partnership models and adhere to those key principles.

21/ Mobile Best Practices, M3AAWG, https://www.m3aawg.org/mobile.

22/ *See e.g.,* CSRIC VII, Working Group 2, "Managing Security Risk in the Transition to 5G,"; CSRIC VII, Working Group 3, "Managing Security Risk in Emerging 5G Implementations," https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii. *See also id.,* CSRIC VII, *Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation* (June 10, 2020).

23/ *A Road Map Toward Resilience Against Botnets*, Nov. 29, 2018, https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_1.pdf.

24/ *See e.g., CISA's ICT Supply Chain Risk Management Task Force Makes Key Acquisition Recommendations* (June 20, 2019), https://www.dhs.gov/news/2019/06/20/cisa-s-ict-supply-chain-risk-management-task-force-makes-key-acquisition; *DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force*, Department of Homeland Security (Oct. 30, 2018), https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology (describing the Task Force's activities, including its function as the industry interface with the C-SCRM program).

Securing network infrastructure, such as 5G, requires a layered approach. It starts with a standards-setting process to ensure the security of the software-driven protocols and algorithms that will underpin new 5G offerings, continues with security by design in product development and deployment, addresses processes and mechanisms for identifying and mitigating vulnerabilities and gaps, promotes effective supply chain security measures, provides interoperability and vendor diversity, and draws upon the NIST Cybersecurity Framework to help effectively manage security risks and threats.

In addition to employing a layered, technology-neutral approach that builds upon existing multi-stakeholder initiatives, the Department also should embrace open security principles in formulating its 5G security strategy. The cable industry has long supported open security principles, including for our wireline networking technologies such as CableLabs' DOCSIS technology, and that these principles are now reflected in the work of groups such as the O-RAN Alliance and appear to hold promise for security and vendor diversity in 5G.[25/] Further, open security not only expedites and refines development of security standards and specs, it promotes competition and vendor diversity by reducing barriers to entry and participation in product design and development.

III. THE DEPARTMENT'S 5G STRATEGY SHOULD PRESERVE AND STRENGTHEN U.S. GLOBAL TECHNOLOGY LEADERSHIP

Technical research and development, product testing, and global standards and specifications around security and interoperability are crucial to bolstering 5G security implementation and innovation. To that end, NTIA, the Department, and Administration should

---

[25/] *See e.g.*, Press Release, *O-RAN Alliance Continues to Grow as Global Operators and Suppliers Reach Across Borders to Collaborate on Open Innovation in Radio Access Networks* (Feb. 20, 2020), https://www.businesswire.com/news/home/20200220005795/en/O-RAN-Alliance-Continues-Grow-Global-Operators-Suppliers.

ensure that their efforts around 5G network security and supply chain promote U.S. global leadership in these areas and do not have the unintended consequence of excluding U.S. companies from participating in international research, development, standards, and specifications work.

In this respect, the Department itself may act on one aspect of a secure 5G strategy, through its rules implementing the directive in Executive Order 13873 to address supply chain risks arising from ICTS. In particular, the Department should ensure that those rules do not inadvertently or unnecessarily impede these critical security-related activities.

The pace of innovation in next-generation wireless systems and infrastructure will continue to accelerate rapidly, and U.S. leadership will depend upon the degree to which companies in the 5G ecosystem can evolve, adapt, and upgrade their network and product features, services, and capabilities. It is therefore critical to continued U.S. leadership in next-generation wireless technologies that the path for ICTS innovation and investment across the wireless ecosystem remain as clear as possible, unencumbered by unnecessary barriers and risks, and that the investors who fund advanced wireless system and infrastructure research, technology development, standards work, deployment, and maintenance are not deterred to the point of diverting their resources to less risky endeavors. Accordingly, to help galvanize 5G infrastructure security innovation and preserve U.S. leadership, the Department should focus the applicability of any rules implementing EO 13873 on transactions that involve actual deployment of 5G ICTS posing material national security risks, and categorically exclude ICTS transactions

that support technical research, testing, and global ICT specifications and standards development.[26/]

The United States is the undisputed world leader in the unlicensed technologies that facilitate efficient use on 4G and 5G wireless networks. American companies are leaders not only in innovation and deployment of these crucial technologies, but also in the standards processes that drive the global unlicensed economy. In the Wi-Fi context, the major chipmakers and OEMs are American companies (e.g., Broadcom, Intel, Qualcomm, HPE, Cisco), who are also heavily involved in standards development. The Wi-Fi standard-setting experience highlights the benefits of strong U.S. company involvement in such efforts, and the Department should pursue policies that fosters a similar outcome for the 5G ecosystem.

The Department's recent decision to amend the rules governing Huawei's placement on the Entity List to clarify that U.S. companies may disclose certain technologies, subject to the Export Administration Regulations (EAR), to standards development bodies in which Huawei is participating should help bolster U.S. leadership on standards and specifications for 5G and other next-generation wireless systems and infrastructure.[27/] Much of this work is done in global forums with international collaboration on technology development. Any new rule in the broader supply chain rulemaking launched by EO 13873 should be harmonized with this decision so that technical standards and specifications, testing and research are not in scope for "transaction" review, and thereby avoid unnecessary hindrance of innovation and new product

---

[26/] *See In the Matter of Securing the Information and Communications Technology and Services Chain*, Docket No. 191119-0084, Comments of NCTA-The Internet & Cable Television Association (Jan. 10, 2020), at 11-12.

[27/] Press Release, *Commerce Clears Way for U.S. Companies to More Fully Engage in Tech Standards-Development Bodies,* Department of Commerce (June 15, 2020), https://www.commerce.gov/news/press-releases/2020/06/commerce-clears-way-us-companies-more-fully-engage-tech-standards. This decision is a step in the right direction of promoting U.S. technology leadership, but the Department should take full account of important standards and specifications developed in organizations that may not readily qualify as a "voluntary consensus standards body" under the current rule.

development. To the extent that transaction review or export control rules hinder U.S. participation in global standard-setting, China would have an increased ability to influence those bodies to further incorporate Chinese technologies, resulting in substantial national security consequences for the United States.

CONCLUSION

For the foregoing reasons, the Department should implement a 5G security strategy reflecting the breadth, diversity, and interdependence of the 5G ecosystem. The strategy should build upon existing security initiatives and frameworks developed via multi-stakeholder processes, promote technology neutrality, embrace open security, and foster vendor diversity. The Department should also preserve and strengthen U.S. global technology leadership by refraining from policies that could inadvertently or unnecessarily hinder participation by American companies in 5G standard setting and technical specifications bodies.

Respectfully submitted,

/s/ Loretta Polk

Matthew J. Tooley
Vice President, Broadband Technology
Science & Technology

Loretta Polk
Danielle Piñeres
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

June 25, 2020