Before the Department of Commerce
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C.

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

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

June 25, 2020

TABLE OF CONTENTS

Before the Department of Commerce
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C.

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

COMMENTS OF CTIA

CTIA[1] welcomes the opportunity to comment on the National Telecommunications and Information Administration's ("NTIA") *Request for Comments* on the Implementation Plan for the *National Strategy to Secure 5G*.[2] CTIA appreciates the Administration's recognition of "the importance of fifth generation wireless technologies ("5G") to the future prosperity and security of the United States[.]"[3]

I. INTRODUCTION AND SUMMARY.

On March 23, 2020, the President signed into law the Secure 5G and Beyond Act of 2020, which required the development of a strategy to ensure the security of next-generation wireless communications systems and infrastructure.[4] On the same day, the Administration published the *National Strategy to Secure 5G,*[5] establishing four lines of effort that the

[1] CTIA-The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Request for Comments, 85 Fed. Reg. 32016 (May 21, 2020) ("*Request for Comments*"), https://www.ntia.doc.gov/files/ntia/publications/fr-secure-5g-implementation-plan-05282020.pdf.

[3] *Id.* at 32017.

[4] *See* Secure 5G and Beyond Act of 2020, Pub L. No. 116-129, 134 Stat. 223 (2020).

[5] *See* THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE 5G OF THE UNITED STATES OF AMERICA (Mar. 2020) ("STRATEGY"), https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

Implementation Plan will follow:

- Facilitating domestic 5G rollout;
- Assessing the cybersecurity risks to and identifying core security principles of 5G capabilities and infrastructure;
- Addressing risks to United States economic and national security during development and deployment of 5G infrastructure worldwide; and
- Promoting responsible global development and deployment of secure and reliable 5G infrastructure.

CTIA responds to NTIA's *Request for Comments* and offers principles to guide "how the U.S. Government can best facilitate the accelerated development and rollout of 5G infrastructure in the United States and with our international partners and lay the groundwork for innovation beyond 5G."[6] The Implementation Plan should:

- Double down to make more spectrum available for exclusive licensed, commercial use;
- Push forward to streamline infrastructure deployment policies;
- Resist proposals to nationalize 5G or pursue top-down government control;
- Harmonize and simplify overlapping efforts on the global supply chain, including emerging regulation of Information and Communications Technology ("ICT") equipment and transactions;
- Protect public-private partnerships as the bedrock of U.S. cybersecurity and 5G strategy;
- Leverage existing private sector collaboration and recommendations on 5G, particularly reports from the President's National Security Telecommunications Advisory Committee's ("NSTAC") and the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC");
- Promote private innovation, including in cybersecurity and Internet of Things ("IoT") certifications and standards;
- Promote broader participation in global standards work, without attempting to control those efforts; and
- Adopt a more strategic and forward-looking approach to include investing in 5G infrastructure, supporting private sector research and development ("R&D"), and pursuing creative and collaborative financing with like-minded allies to promote

[6] *Request for Comments* at 32017.

vendor diversity and respond to other countries' industrial policy.

By including these principles and avoiding unnecessary regulation, the federal government can help cement America's leadership and accelerate the transition to secure 5G.

II. 5G WILL BE TRANSFORMATIVE, MAKING OUR LIVES BETTER, COMMUNITIES SAFER, AND THE NATION MORE PROSPEROUS.

A. Industry-Led 5G Deployments Will Spur Enormous Economic Growth and Should be the Centerpiece of Implementing the *National Strategy to Secure 5G.*

5G will power an explosion of innovation and jobs, boosting the U.S. economy and transforming numerous industries. 5G will play a vital role towards the prosperity and security of the United States. 5G supports more diverse applications and more connections with greater capacity, lower latency, and increased speed. These networks will handle exponential growth in demand for capacity, connectivity, and capability—delivering a better, faster experience for all.[7] Shifting to 5G will positively impact myriad industries, including agriculture, commerce, healthcare, transportation, smart cities, education, manufacturing, energy, and more.[8] The 5G mobile value chain alone could generate up to $3.6 trillion in revenue by 2035 and support more than 22.4 million jobs globally, of which $768 billion in revenue and 2.8 million jobs will be in the United States.[9] The "skyrocketing popularity of streaming services and wireless earbuds

[7] *See The 5G Economy*, CTIA, https://www.ctia.org/the-wireless-industry/the-5g-economy (last visited June 19, 2020).

[8] *See* Don Reisingner, *How 5G Promises to Revolutionize Farming*, FORTUNE (Feb. 28, 2020), https://fortune.com/2020/02/28/5g-farming/; DELOITTE, WIRELESS CONNECTIVITY FUELS INDUSTRY GROWTH AND INNOVATION IN ENERGY, HEALTH, PUBLIC SAFETY, AND TRANSPORTATION (Jan. 2017), https://api.ctia.org/docs/default-source/default-document-library/deloitte_2017011987f8479664c467a6bc70ff0000ed09a9.pdf; *How 5G Will Advance Educational Technology on Campus*, EDTECH (Jan. 16, 2020), *available at* https://edtechmagazine.com/higher/article/2020/01/how-5g-will-advance-educational-technology-campus; Enno de Boer et. Al, *Five Ways that 5G Will Revolutionize Manufacturing*, MCKINSEY & COMPANY, (Oct. 18, 2019), https://www.mckinsey.com/business-functions/operations/our-insights/operations-blog/five-ways-that-5g-will-revolutionize-manufacturing#:~:text=5G%20speeds%20up%20the%20decision,running%20and%20prices%20are%20favorable./.

[9] *See* CTIA, IN THE MATTER OF OFFICE OF ECONOMICS AND ANALYTICS SEEKS COMMENT ON THE STATE OF COMPETITION IN THE COMMUNICATIONS MARKETPLACE 58 (Apr. 27, 2020) ("CTIA MARKETPLACE REPORT"),

along with 5G connectivity and artificial intelligence ("AI")-enabled devices will drive revenue growth for the U.S. consumer tech industry to a record $422 billion in retail revenues in 2020."[10]

Driven by intense competition in the wireless market, national wireless providers have already begun aggressive 5G deployment plans.[11] Verizon now offers 5G Ultra Wideband service, leveraging its millimeter wave spectrum, in parts of 35 cities, and they are looking to almost double it, growing it to almost 60 cities by the end of the year,[12] along with additional successful trials putting them on track to launch 5G nationwide in 2020.[13] AT&T's 5G offering appears in more than 327 markets and covers more than 160 million people,[14] along with mobile Millimeter Wave ("mmWave") 5G in parts of 35 cities,[15] and will have a nationwide 5G network running on low-band spectrum later this summer. T-Mobile launched its 5G network nationwide in 2019, covering nearly 6,000 towns and more than 225 million people.[16] Regional and rural carriers area already launching 5G or planning for deployment. U.S. Cellular has launched 5G service in dozens of cities in Iowa and Wisconsin,[17] and new entrants like DISH are poised to

https://ecfsapi.fcc.gov/file/1042775336755/200427%20CTIA%20Comments%20for%20Communications%20Marketplace%20Report.pdf.

[10] Danielle Cassagnol, *Consumer Tech U.S. Sales to Reach Record $422 Billion in 2020; Streaming Services Spending Soars, Says CTA*, CONSUMER TECH. ASS'N (Jan. 5, 2020), https://www.cta.tech/Resources/Newsroom/Media-Releases/2020/January/Consumer-Tech-U-S-Sales-to-Reach-Record-$422-B-(1).

[11] *See* CTIA MARKETPLACE REPORT.

[12] *See* Aaron Pressman, *Verizon to double the number of cities with its 5G mobile service this year*, Forbes (Feb. 13, 2020) https://fortune.com/2020/02/13/verizon-5g-mobile-network-double-number-of-cities/.

[13] *See* Kelly Hill, *Verizon completes DSS tests, on track to activate this year*, RCR Wireless (June 23, 2020) https://www.rcrwireless.com/20200623/5g/verizon-completes-dss-tests-on-track-to-activate-this-year.

[14] *See* AT&T, *AT&T 5G Launches in 137 New Markets, Covering More Than 160 Million People in the U.S.* (June 15, 2020) https://about.att.com/newsroom/2020/5g_announcements.html.

[15] *See* AT&T, *5G*, https://about.att.com/pages/5G (last visited June 19, 2020).

[16] *See* T-Mobile, *T-Mobile 5G Factsheet* (May 2020) https://www.t-mobile.com/content/dam/t-mobile/corporate/newsroom/articles/2020/05/connecting-heroes/T-Mobile-5G-Factsheet-May-2020.pdf.

[17] *See e.g.* Leah Jones, *U.S. Cellular Turn on 5G Network for Eastern Iowa Customers* (Mar. 6, 2020) https://www.radiokeokuk.com/2020/03/u-s-cellular-turns-on-5g-network-for-eastern-iowa-customers/#:~:text=Burlington%2C%20Cedar%20Rapids%2C%20Coralville%2C,the%20U.S.%20Cellular%205G

enter the marketplace,[18] helping to fill the gaps in broadband access in rural areas.

In 2020 and beyond, these networks will continue to evolve with new use cases, even more expansive network rollouts, and innovative technologies, which together will fuel America's 5G economy.[19] As the Administration predicted, the market for 5G devices and services is growing exponentially.[20] Device manufacturers continue to roll out devices to meet the pressing demands of consumers.[21] Wireless use in the United States continues to grow at an exponential rate, and handset manufacturers like Samsung, Motorola, and LG already are introducing 5G devices in the United States. Wireless original equipment manufacturers ("OEMs") are producing new 5G-oriented solutions and innovations, like Ericsson's smart factory. IoT solutions, for uses in smart cities and smart infrastructure solutions, are forthcoming.

B. America's 4G Experience Demonstrates Why the *National Strategy to Secure 5G* Must Promote Innovation, Collaboration, and Light-Touch Regulatory Policy.

The United States should continue to pursue leadership in 5G and evolving communications technology, having seen the rewards of 4G dominance. Building upon America's 4G leadership, as of 2018, the wireless industry supported over 4.7 million jobs and contributed roughly $475 billion annually to the U.S. economy.[22] A study performed by Recon

%20network; Erica Dynes, *Reedsburg among first cities in state to access U.S. Cellular 5G Network* (Mar. 9, 2020) https://www.wiscnews.com/reedsburgtimespress/news/local/reedsburg-among-first-cities-in-state-to-access-u-s/article_8f69f88e-801d-509f-b37d-6f775f8d5338.html.

[18] *See* CTIA MARKETPLACE REPORT at iii–iv.

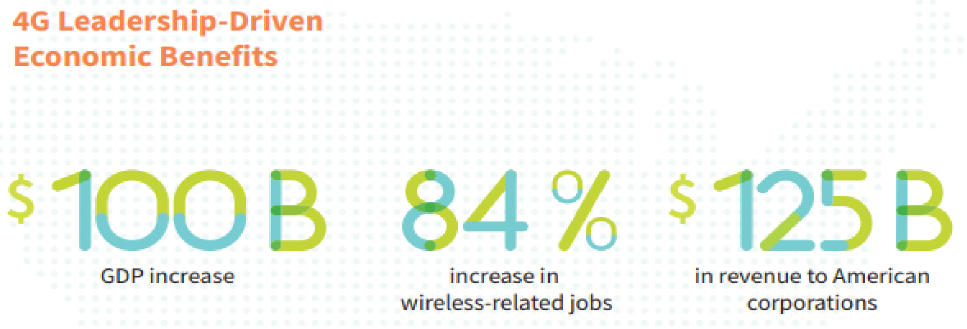
[19] *See* Tom Sawanobori, *Wireless in 2020: The 5G Economy Roars to Life*, CTIA (Dec. 21, 2019), https://www.ctia.org/news/wireless-in-2020-the-5g-economy-roars-to-life.

[20] *See* THE WHITE HOUSE, EMERGING TECHNOLOGIES AND THEIR EXPECTED IMPACT ON NON-FEDERAL SPECTRUM DEMAND 1 (May 2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/Emerging-Technologies-and-Impact-on-Non-Federal-Spectrum-Demand-Report-May-2019.pdf.

[21] *See* CTIA MARKETPLACE REPORT at 3–8.

[22] *See U.S. Wireless Industry Contributes $475 Billion Annually to America's Economy and Supports 4.7 Million Jobs, According to New Report*, ACCENTURE (Apr. 5, 2018), https://newsroom.accenture.com/news/us-wireless-

Analytics found that America's leadership on 4G resulted in a range of benefits:



Source: RACE TO 5G REPORT, CTIA 4 (2018), https://www.ctia.org/news/race-to-5g-report.

The United States should heed lessons from other nations that forfeited wireless leadership in 3G and 4G, and experienced long-term negative effects. Europe led in 2G and Japan led in 3G. Losing that leadership in subsequent generations resulted in massive job losses and a contraction of the regions' telecom hardware and software industries. According to the European Commission's spokesman for digital economy, in the "mobile equipment industry, we had 80 percent of the market in 2008 and because we were not ready for 4G mass deployment, the European industry lost almost its entire market share for mobile phones."[23]

The United States has prioritized 5G leadership. As a White House Report aptly stated:

> Through investment in R&D for next generation capabilities, ensuring efficient allocation and use of spectrum, and removing regulatory barriers, the Government plays a critical role in 5G deployment. Through such an approach, we can maintain our Nation's global leadership in wireless technologies and the industries of the future.[24]

Leading the 5G economy will require a steady pipeline of spectrum auctions and continued

industry-contributes-475-billion-annually-to-americas-economy-and-supports-4-7-million-jobs-according-to-new-report.htm.

[23] RACE TO 5G REPORT, CTIA 5 (Apr. 2018), https://www.ctia.org/news/race-to-5g-report.

[24] THE WHITE HOUSE, EMERGING TECHNOLOGIES AND THEIR EXPECTED IMPACT ON NON-FEDERAL SPECTRUM DEMAND 1 (May 2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/Emerging-Technologies-and-Impact-on-Non-Federal-Spectrum-Demand-Report-May-2019.pdf.

modernization of infrastructure siting rules. These are the pillars of wireless regulatory policy that will drive continued deployment and innovation in 5G.[25]

As it pushes forward, the United States should resist ill-formed proposals to nationalize control of U.S. networks, as well as heavy-handed top-down regulation. As CTIA explained in lauding the President's commitment to private leadership in 5G:

> The White House's continued commitment to the free-market principles that have made the U.S. the global leader in wireless recognizes this industry's remarkable track record of investing in our nation's connectivity infrastructure—$226 billion in the last nine years alone.[26]

The federal government should also avoid selecting, acquiring large stakes in, or backing individual companies or entities. This will only accelerate vendor consolidation, lead to government-sanctioned monopolies, complicate those organizations' roles in the international marketplace, and reduce innovation. The United States should promote competition and diversity in the supply chain through R&D and by making the United States a desirable place for technology investment. Market-driven innovation should be a bedrock principle of the nation's 5G strategy.

C. No Sector Has More at Stake Than the Mobile Ecosystem, Which is Addressing 5G Security in Global Standards Bodies and in Collaboration With Government in Venues From CSCC, CSRIC, the NSTAC, and More.

The President's *National Strategy to Secure 5G* committed to "continue to work aggressively with the private sector" on 5G. The structures to do so are in place and ready.

Drawing on decades of layered security, every part of the mobile ecosystem is playing its

[25] *See* THE GLOBAL RACE TO 5G: SPRING 2019 UPDATE, CTIA (Apr. 2019), https://api.ctia.org/wp-content/uploads/2019/04/The-Global-Race-to-5G-Spring-2019-Update.pdf.

[26] Meredith Attwell Baker, *CTIA Statement on White House 5G Commitment*, CTIA (Apr. 12, 2019), https://www.ctia.org/news/ctia-statement-on-white-house-5g-commitment.

role. From individual members' security innovations, to CTIA's Cybersecurity Working Group, to partnerships with federal agencies, to activity in the Alliance for Telecommunications Industry Solutions ("ATIS") and the 3rd Generation Partnership Project ("3GPP"), the entire ecosystem is focused on security in our 5G future. The recent CSRIC VII, Working Group 2 report details numerous private and collaborative security efforts.[27]

The U.S. Communications Sector Coordinating Council ("CSCC") works with industry participants "to improve the physical and cyber security of sector assets; ease the flow of information within the sector, across sectors and with designated federal agencies; and address response and recovery following an incident or event."[28] CSCC works with the Department of Homeland Security's ("DHS") National Risk Management Center ("NRMC"), the Cybersecurity and Infrastructure Security Agency ("CISA") and other agencies, with which industry actively collaborates.

The FCC's CSRIC has been a years-long, vital partnership that enables in-depth study and development of best practices for discrete challenges. CSRIC brings together industry and government to examine numerous aspects of telecommunications and Internet security, including multiple aspects of 5G.[29] The FCC's Technology Advisory Council ("TAC") has been providing technical advice to the agency on 5G and IoT, spectrum, antenna advances, and artificial

[27] *See* CSRIC WORKING GROUP 2: MANAGING SECURITY RISK IN THE TRANSITION TO 5G, REPORT ON RISKS TO 5G FROM LEGACY VULNERABILITIES AND BEST PRACTICES FOR MITIGATION (June 2020), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii.

[28] *About the CSCC*, U.S. COMMC'NS SECTOR COORDINATING COUNCIL, https://www.comms-scc.org/about-1 (last visited June 19, 2020).

[29] *See Communications Security, Reliability, and Interoperability Council VII*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii (last visited June 19, 2020).

intelligence.[30]

The NSTAC has tackled 5G and Internet security and has been tasked with providing the President with the best possible industry advice related to the nation's critical national security and emergency preparedness challenges.[31]

The National Institute for Standards and Technology ("NIST") and its National Cybersecurity Center of Excellence ("NCCoE") have been doing important work on 5G security, in coordination with the communications sector's expertise on security issues.[32]

A coordinated approach to 5G that harmonizes current work and champions market forces, public-private partnerships, and global engagement is critical.

III. SEVERAL POLICY IMPERATIVES WILL FACILITATE THE RAPID ROLLOUT OF 5G IN THE UNITED STATES (LINE OF EFFORT ONE).

In the *Request for Comments*, Line of Effort One asks how to facilitate the domestic rollout of 5G.[33] To support deployment of 5G, the Implementation Plan should:

- Promote policies to support commercial access to licensed, exclusive flexible-use spectrum to support wireless connectivity, including 5G;
- Streamline and modernize infrastructure deployment processes;
- Create consistent national regulatory environments, including for privacy; and
- Support R&D in real-world use cases and encourage private sector participation in standards efforts, ensuring a diverse 5G supply chain.

[30] *See Technological Advisory Council*, FED. COMMC'NS COMM'N, https://www.fcc.gov/general/technological-advisory-council (last visited June 19, 2020).

[31] *See National Security Telecommunications Advisory Committee*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, (Nov. 21, 2018), https://www.cisa.gov/national-security-telecommunications-advisory-committee.

[32] *See, e.g. See Preparing a Secure Evolution to 5G*, NAT'L CYBERSECURITY CTR. OF EXCELLENCE, https://www.nccoe.nist.gov/projects/building-blocks/5g-secure-evolution (last visited June 19, 2020).

[33] NTIA asks how can the U.S. government "best facilitate the domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem?"; how can "the U.S. Government best foster and promote the research, development, testing, and evaluation of new technologies and architectures?"; what "steps can the U.S. Government take to further motivate the domestic-based 5G commercial ecosystem to increase 5G research, development, and testing?" and what "areas of research and development should the U.S. Government prioritize to achieve and maintain U.S. leadership in 5G?" *Request for Comments* at 32017.

A. The Federal Government Should Double Down on Smart Spectrum Policy.

Spectrum is the critical input for wireless service. Wireless carriers need a pipeline of low-, mid-, and high-band spectrum to make 5G deliver very high speed, low latency capabilities nationwide. Freeing up additional airwaves for exclusive, licensed use will help providers meet skyrocketing consumer demand and deliver our 5G future.[34]

U.S. policymakers have recognized the importance of spectrum in the race to 5G and have identified key future spectrum opportunities. CTIA supports the FCC's plans to auction 280 megahertz of spectrum in the C-band in December 2020, and its commitment to auction another 70 megahertz in the 3.5 GHz CBRS band this summer.[35] For the C-band in particular, once the winning bidders are identified, avoiding delays in post-auction relocations and the issuance of licenses to winning bidders will be critical. Moreover, although the CBRS spectrum that the Commission plans to auction will bring its own unique challenges (*e.g.*, power levels that are broadly recognized to be too low), this auction nevertheless presents an opportunity for stakeholders to innovate. Still, policymakers need to continue efforts to identify additional spectrum to bring to market, particularly in the mid-band range.[36]

To ensure U.S. leadership in 5G, wireless carriers specifically need commercial access to additional licensed mid-band spectrum. Mid-band spectrum is essential for 5G because it combines very high capacity and throughput with good propagation characteristics, providing coverage across widespread areas and within buildings. A robust spectrum pipeline that includes

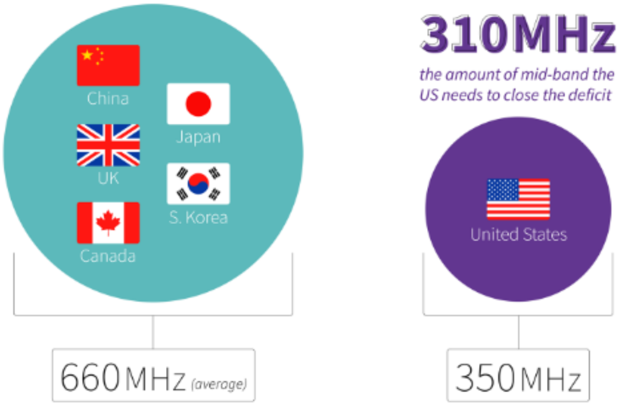
[34] *See The 5G Economy*, CTIA, https://www.ctia.org/the-wireless-industry/the-5g-economy (last visited June 19, 2020).

[35] *See* Letter from Meredith Attwell Baker, President and CEO, CTIA, to the Honorable Roger Wicker et. al., at 1 (Feb. 25, 2020), https://api.ctia.org/wp-content/uploads/2020/02/MidBand-Letter-2-25-20.pdf.

[36] *See* THE GLOBAL RACE TO 5G: SPRING 2019 UPDATE, CTIA (2019), https://api.ctia.org/wp-content/uploads/2019/04/The-Global-Race-to-5G-Spring-2019-Update.pdf.

ample mid-band spectrum for licensed operations will be crucial to ensuring that wireless providers can usher in the 5G economy with its resulting jobs creation and economic growth.

While America ranks strongly in the majority of 5G-readiness metrics, China and other countries are ahead in making critical mid-band spectrum available for 5G.[37] A recent Analysys Mason report surveyed the amount of mid-band spectrum (3 GHz-7 GHz) available, as well as the amount expected to be available by the end of 2020 and 2022, in 14 countries.[38] By the end of 2022, the report concluded, five countries will make nearly twice the amount of mid-band spectrum available for commercial wireless use as the U.S.:



Source: *5G Mid-Band Spectrum Global Update*, CTIA, https://www.ctia.org/news/report-5g-mid-band-spectrum-global-update (last visited June 19, 2020).

The United States needs to effectively double its licensed mid-band spectrum to keep pace with leading nations. Beyond the auctions that are already scheduled for 2020, the Administration should work collaboratively with the FCC to explore opportunities to use the Lower 3 GHz band

[37] *See Id.*

[38] *See* JANETTE STEWART ET. AL., 5G MID-BAND SPECTRUM GLOBAL UPDATE ANALYSYS MASON (Mar. 2020), https://www.ctia.org/news/report-5g-mid-band-spectrum-global-update.

for licensed, exclusive use.[39]

In addition to critical mid-band spectrum, a mix of low- and high-band spectrum will also be needed to support 5G deployments. Whereas low-band spectrum has long wavelengths and can travel long distances, high-band spectrum has greater capacity but limited range. The FCC's efforts in transitioning the 600 MHz band[40] and auctioning nearly five gigahertz of millimeter wave spectrum[41] enabled the U.S. to roll out 5G before its global counterparts.

In sum, the Administration should continue to emphasize key fundamentals:

- Create and execute on a schedule of auctions that makes more spectrum—especially mid-band spectrum—available for exclusive, licensed wireless use;[42]
- Recommit federal spectrum policy to proven free-market approaches that harness the power of competition to enhance our nation's economic and national security;
- Modernize government policies and procedures to ensure optimal use of spectrum; and
- Help harmonize spectrum decisions globally. The U.S. government must amplify and protect its spectrum decisions by promoting international harmonization of 5G spectrum so that carriers can take advantage of economies of scale and global roaming.

B. The Nation Should Continue to Modernize its Infrastructure Policy.

Every level of government has a role in modernizing infrastructure siting rules.[43] CTIA and its members applaud the progress in this area[44] and encourage more action. As exemplified

[39] *See* CTIA MARKETPLACE REPORT at 62.

[40] *See Auction 1002 Long-form Applications Granted*, FED. COMMC'NS COMM'N, https://www.fcc.gov/document/auction-1002-long-form-applications-granted-3.

[41] *See FCC Takes Steps to Make Millimeter Wave Spectrum Available for 5G*, FED. COMMC'NS COMM'N (Apr. 12, 2019), https://www.fcc.gov/document/fcc-takes-steps-make-millimeter-wave-spectrum-available-5g.

[42] *See* THE GLOBAL RACE TO 5G: SPRING 2019 UPDATE, CTIA (2019), https://api.ctia.org/wp-content/uploads/2019/04/The-Global-Race-to-5G-Spring-2019-Update.pdf.

[43] *See* RACE TO 5G REPORT, CTIA 13 (2018), https://www.ctia.org/news/race-to-5g-report.

[44] *See, e.g.*, The FCC's *5G FAST Plan*, FED. COMMC'N COMM'N, https://www.fcc.gov/5G (last visited June 19, 2020).

in the MOBILE NOW Act,[45] the 2012 Spectrum Act, and provisions in the Communications Act adopted over decades, Congress has consistently made the rapid, efficient deployment of wireless infrastructure a national priority.

NTIA should be applauded for recent streamlining efforts, as envisioned in the American Broadband Initiative. These include reforms to offer permitting processes online and develop tools to identify eligible federal assets for deployment. NTIA and federal agencies should support additional reforms, including implementation of the MOBILE NOW Act's 270-day shot clock for reviews of siting on federal lands and properties. The federal government can continue to streamline siting processes for federal land and property. This will allow spectrum resources to be used in even more remote areas and regions of the country.

NTIA should also work with the Federal Aviation Administration ("FAA"), the FCC, wireless service providers, and tower owners to update the FAA's "Collocation Void" ("Colo Void") Policy, and develop a plan for future amendments as new commercial spectrum is allocated. In 2007, the FAA revised and updated its electromagnetic interference ("EMI") evaluation processes for existing structures to make clear that entities are not required to file notice with the FAA for an aeronautical study simply to add frequencies in certain bands to an existing structure that has a current No Hazard Determination.[46] This policy has had immediate and long-lasting benefits, enabling additional antennas to be collocated on existing structures, and enabling expanded and improved service to consumers. This relief, however, has been limited to the particular transmitting frequencies listed in the November 2007 publication, which does not include the bands made available by the FCC for commercial use in the subsequent 13

[45] *See* Consolidated Appropriations Act, Pub. L. No. 115-141, § 601, 132 Stat. 348 (2018).

[46] *See* Colo Void Clause Coalition; Antenna Systems Co-Location; Voluntary Best Practices; Docket No. FAA-2004-16982; Notice No. 07-16, 72 Fed. Reg. 65449 (Nov. 21, 2007).

years. Like the frequency bands on the approved Colo Void list, these new bands will be used to deliver services that are highly unlikely to raise EMI concerns. The addition of these frequency bands and technologies to the approved list would thus be of great public benefit, allowing the expeditious buildout of new wireless services throughout the country, while conserving scarce administrative resources.

The FCC has likewise been a faithful steward of this national policy. The Commission has taken concrete actions over the past few years to accelerate 5G by removing regulatory barriers that impede deployment. In 2018, for instance, the FCC provided guardrails regarding state, local, and historic preservation review processes, and clarified its rules where necessary to promote greater predictability in siting reviews. Smart infrastructure policies at the federal and state levels are speeding deployment across the country. As FCC Commissioner Brendan Carr has explained, "smart infrastructure policies . . . can flip the business case for thousands of communities."[47] The FCC's 5G Upgrade Order, adopted in June 2020, also will advance the long-standing bipartisan consensus to give wireless providers greater flexibility to upgrade existing facilities with next-generation infrastructure critical to American leadership in the emerging 5G economy.[48]

While these federal policies are critical, state and local actions are similarly important. Forward-thinking states and localities have changed their laws to facilitate deployment, including by setting clear timelines and cost-based rates for infrastructure reviews. Such actions—rather than further obstacles to deployment—should be encouraged in order to bring enhanced coverage

[47] COMMISSIONER BRENDAN CARR, FED. COMMC'N COMM'N, KEYNOTE ADDRESS AT THE INTERNATIONAL INSTITUTE OF COMMUNICATIONS 2019 TELECOMMUNICATIONS AND MEDIA FORUM: BUILDING A 5G WORLD (Dec. 10, 2019), https://docs.fcc.gov/public/attachments/DOC-361292A1.pdf.

[48] *See* Meredith Attwell Baker, CTIA Statement on Commissioner Carr's 5G Upgrade Proposal, CTIA (May 19, 2020), https://www.ctia.org/news/ctia-statement-on-commissioner-carr-5g-upgrade-proposal.

and capacity to Americans across the country and prepare networks to accommodate future technologies.

C. The Federal Government Should Promote Consistent National Regulatory Environments, Including for Privacy.

Wireless consumers deserve robust consumer protections. One way to do that is by setting permanent, common-sense federal regulations for interstate services like mobile broadband. Innovation and investment in tomorrow's networks also need promotion to ensure an open Internet and protect consumer privacy.[49]

A federal law would also ensure that state broadband regulations do not contravene federal policies, undercut investment, or slow wireless deployment. Crossing state lines does not change a consumers' mobile experience. The laws governing that experience should not change either.[50] The 5G economy could also be hampered by diffuse and overlapping state-level privacy and security regulations. Complex and unaligned frameworks threaten to limit innovation and make it harder to offer services and use data across state lines.[51]

CTIA supports "uniform, national privacy standards across the digital economy, enshrined by Congress in federal law and enforced by the Federal Trade Commission."[52] A reliable, uniform regulatory framework will protect consumers while facilitating investment in

[49] *See The 5G Economy*, CTIA, https://www.ctia.org/the-wireless-industry/the-5g-economy (last visited June 19, 2020).

[50] *See Positions; Net Neutrality*, CTIA, https://www.ctia.org/positions/net-neutrality (last visited June 19, 2020).

[51] *See, e.g.*, Len Cali, Senior VP of Public Policy, *A Broad Consensus for Federal Privacy Legislation*, AT&T PUB. POLICY (Sept. 28, 2018), https://www.attpublicpolicy.com/privacy/a-broad-consensus-for-federal-privacy-legislation/; Chris Boyer, Assistant VP of Global Public Policy, *Developing an Effective Cybersecurity Strategy for the Entire Internet Ecosystem*, AT&T PUB. POLICY (Nov. 6, 2017), https://www.attpublicpolicy.com/administration/developing-an-effective-cybersecurity-strategy-for-the-entire-internet-ecosystem/.

[52] Kelly Cole & Tom Power, *Protecting Consumers with Federal Privacy Legislation*, CTIA (Nov. 9, 2018), https://www.ctia.org/news/protecting-consumers-with-federal-privacy-legislation#:~:text=CTIA%20supports%20legislation%20that%20requires,that%20information%20may%20be%20shared.

next-generation networks and services, and enabling the mobile ecosystem to do what it does best: empower Americans' mobile and connected lives.

D. Federal Research and Development Should Focus on Supplementing Private Investment as One Aspect of More Strategic Global Positioning.

As described below, the federal government is pursuing R&D to test 5G and develop best practices, but the United States needs to think bigger about investing in 5G innovations, including working with like-minded countries. Currently, NCCoE has started a project to "showcase the practical 5G cybersecurity capabilities provided by the 5G system and complementing technology."[53] The DoD has launched solicitations, in coordination with the National Spectrum Consortium, for a series of requests for prototype proposals ("RPPs") to help pave the way for incorporating 5G technologies into military networks.[54] National labs play a role too, including the Idaho National Lab, which launched the Wireless Security Institute to lead and coordinate government, academic, and private industry research efforts, fostering more secure and reliable 5G wireless technology.[55] While these activities can be helpful for the future of 5G, coordination among the various efforts is essential. CTIA and its members encourage NTIA to look at the growing government R&D and grants in 5G to ensure that work is not duplicative and that it focuses on real-world, practical use cases.

[53] MIKE BURTOK ET. AL., NAT'L CYBERSECURITY CTR. FOR EXCELLENCE, 5G CYBERSECURITY: PREPARING A SECURE EVOLUTION TO 5G 5 (Apr. 2020), https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/5G-pse-project-description-final.pdf.

[54] *See* Jared Serbu, *Pentagon Releases Last of Four Solicitations To Test 5G Technologies*, FED. NEWS NETWORK (Apr. 9, 2020), https://federalnewsnetwork.com/on-dod/2020/04/pentagon-releases-last-of-four-solicitations-to-test-5g-technologies/.

[55] *See Wireless Security Institute Established at Idaho National Laboratory To Improve 5G Technology*, Idaho Nat'l Lab. (Oct. 2, 2017), https://inl.gov/article/wireless-security-institute-established-at-idaho-national-laboratory-to-improve-5g-technology/.

5G network security is being addressed in standards bodies and in private R&D to test use cases and verify the functionality of 3GPP standards and other work. The government should support private R&D and testing nationwide.

Security efforts are crucial to the future of 5G, and carriers are leading the charge with cutting edge research. AT&T maintains partnerships with Purdue Research Lab[56] and its AT&T Foundry is engaged in six cities across the globe,[57] T-Mobile's Launch Pad opened a 5G device lab;[58] Verizon maintains 5G Labs for collaboration in New York City, Washington D.C., Cambridge (MA), Los Angeles, and Palo Alto (CA).[59] There is also a 5G First Responder Lab[60] and WarnerMedia has an Innovation Lab.[61]

CTIA launched a first-of-its-kind *IoT Security Certification*, which augments its existing testing and certification offerings for the mobile ecosystem. The cybersecurity certification program for IoT devices establishes an industry baseline for device security on wireless networks. It supports a variety of use cases and levels of device sophistication.[62] Underwriters Laboratories ("UL") maintains a 5G device testing offering, to evaluate the safety, connectivity, and performance of devices operating on sub-6 GHz and mmWave frequencies to global

[56] *See Purdue University's College of Engineering Accelerates Research and Innovation with AT&T 5G at Indiana 5G Zone*, AT&T (Nov. 21, 2019), https://about.att.com/story/2019/att_purdue_5g.html.

[57] *See* AT&T FOUNDRY, https://foundry.att.com/ (last visited June 19, 2020).

[58] *See Built for the 5G Future: T-Mobile Opens New Device Lab*, T-MOBILE (Aug. 20, 2019), https://www.t-mobile.com/news/5g-device-lab.

[59] *See* VERIZON 5G LABS, https://verizon5glabs.com/ (last visited June 19, 2020).

[60] *See* 5G FIRST RESPONDER LAB, https://www.5gfirstresponderlab.com/ (last visited June 19, 2020).

[61] *See Introducing the WarnerMedia Innovation Lab*, WARNER MEDIA (Jan. 22, 2019) https://www.warnermediagroup.com/blog/posts/20190122-introducing-the-warnermedia-innovation-lab.

[62] *See Certification Resources*, CTIA, https://www.ctia.org/about-ctia/programs/certification-resources (last visited June 19, 2020).

regulatory and industry requirements,[63] and the Council for Securing the Digital Economy brings together companies from across the ICT sector to develop a set of IoT device security guidelines,[64] to name just a few examples.

The federal government should encourage these and other efforts, including 5G test beds that partner with the private sector.[65] Private test beds are vital to understanding the real-world impacts of 5G networks, devices, and applications. These partnerships should be encouraged, particularly to focus on real world and commercially-viable approaches and should be based in the templates underway at DHS CISA,[66] NIST,[67] and the NCCoE.[68]

According to the NSTAC *Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem*, "[t]he Government must seek to foster the conditions in which the companies that develop and produce current and future technology upon which [National Security/Emergency Preparedness ("NS/EP")] depends can thrive."[69] AT&T has observed that "[a]s many western countries are

[63] *See 5G Compliance Testing*, UNDERWRITERS LABS., https://www.ul.com/offerings/5g-compliance-testing (last visited June 19, 2020).

[64] *See, e.g., International Botnet and IoT Security Guide*, COUNCIL TO SECURE THE DIGITAL ECON., https://securingdigitaleconomy.org/projects/international-anti-botnet-guide/ (last visited June 19, 2020); *The C2 Consensus on IoT Security Baseline Capabilities*, COUNCIL TO SECURE THE DIGITAL ECON., https://securingdigitaleconomy.org/projects/c2-consensus/ (last visited June 19, 2020).

[65] *See, e.g., FCC Establishes First Two Innovation Zones*, FED. COMMC'NS COMM'N (Sept. 16, 2019), https://docs.fcc.gov/public/attachments/DOC-359737A1.pdf.

[66] *See Information and Communications Supply Chain Risk Management Task Force*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (June 15, 2020), https://www.cisa.gov/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

[67] *See NIST Helps Build Accurate Measurement Infrastructure for 5G Communications*, NAT'L INST. OF STANDARDS AND TECH. (Mar. 18, 2020), https://www.nist.gov/news-events/news/2020/03/nist-helps-build-accurate-measurement-infrastructure-5g-communications.

[68] *See Preparing a Secure Evolution to 5G*, NAT'L CYBERSECURITY CTR. OF EXCELLENCE, https://www.nccoe.nist.gov/projects/building-blocks/5g-secure-evolution (last visited June 19, 2020).

[69] NAT'L SEC. TELECOMMS. ADVISORY COMM., REPORT TO THE PRESIDENT ON ADVANCING RESILIENCY AND FOSTERING INNOVATION IN THE INFORMATION AND COMMUNICATIONS TECHNOLOGY ECOSYSTEM 3 (2019) ("NSTAC REPORT"),

cutting back on government-encouraged research and development, China is making substantial investments. The United States should carefully consider what role it wants domestic industry and innovation to play in long-term technology leadership and standards development, and how to ensure that the incentives for R&D are in place."[70]

United States R&D should be part of a broader strategy that considers partnerships with allies and trusted private sector partners, as discussed in more detail below. The government has received important recommendations about fostering investment. The NSTAC Report outlined steps the government can take to foster "the conditions that sustain key manufacturing capabilities and capacity in the face of unfair foreign support and to keep the United States on the forefront of innovation, to the greatest extent possible, in strategically important areas of technology."[71] Recommended steps include to:

- Adopt policies that encourage new companies to enter key technology sectors and markets or for companies in existing markets to remain.
- Improve existing mechanisms for collaboration on national strategic priorities with the manufacturing and innovation communities and the critical sectors.
- Expand initiatives that encourage U.S. companies to innovate. Encourage U.S. companies and universities to create patents for their new ideas and inventions. These are important to help ensure the U.S. is at the forefront of innovation.
- Encourage innovation community stakeholders to build strong security into products and to factor national security imperatives into their decision-making.
- Collaborate more closely with business executives within the critical sectors to ensure that they know the true risk of relying on ICT that could be compromised and under the influence of adversarial foreign nations.[72]

Each of these efforts will help promote domestic deployment of 5G and future generations.

https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_0.pdf.

[70] AT&T, 5G POLICY PRIMER: THE GLOBAL STANDARDS PROCESS IS ROBUST AND EFFECTIVE IN ADVANCING U.S. GOALS 9 (2020), https://policyforum.att.com/wp-content/uploads/2020/03/5G-Standards-Whitepaper-March-2020.pdf.

[71] NSTAC REPORT at 3.

[72] *Id.* at 4.

IV. INDUSTRY HAS BEEN IDENTIFYING RISKS AND BUILDING SECURITY IN 5G INFRASTRUCTURE (LINE OF EFFORT TWO).

The *Request for Comments* seeks feedback on the second line of effort: building security into 5G infrastructure.[73] Security is being built into 5G networks from the ground up.

A. The U.S. Government Should Consider Security Enhancements in 5G Networks and Devices as It Develops Security Principles for 5G Infrastructure.

Major security advancements are baked into 5G technologies and the networks that will support 5G. As operators deploy 5G, "they are aggressively building in security and are structuring networks in a distributed manner that virtualizes functions so that critical functions can be processed at the network's edge in near real-time."[74] As CSRIC explains, "[t]here are a number of enhancements made in 5G specifications to provide increased security as compared to 3G and 4G."[75]

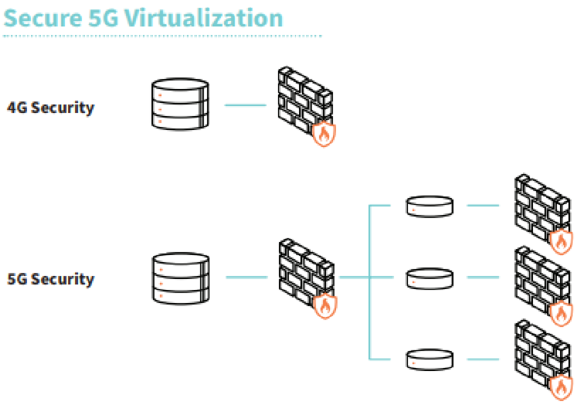
Software Defined Networks ("SDNs") and Network Function Virtualization ("NFV") are additional key features that allow operators to deploy and manage a more flexible, scalable, and powerful core network, and will enable enhanced security features in 5G. Network operators have been moving from a hardware-centric network design methodology to one that is software-centric.[76] SDN, in effect, gives network operators centralized control over the network, and NFV allows software to build and operate the network.

[73] *See Request for Comments* at 32017.

[74] AT&T, 5G POLICY PRIMER: FUTURE WIRELESS NETWORKS WILL HAVE UNPRECEDENTED SECURITY 1 (2018), https://policyforum.att.com/wp-content/uploads/2018/11/5G_Security_1.pdf.

[75] *See* CSRIC WORKING GROUP 2: MANAGING SECURITY RISK IN THE TRANSITION TO 5G, REPORT ON RISKS TO 5G FROM LEGACY VULNERABILITIES AND BEST PRACTICES FOR MITIGATION, 22 (June 2020). https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii.

[76] NSTAC REPORT at A-5.



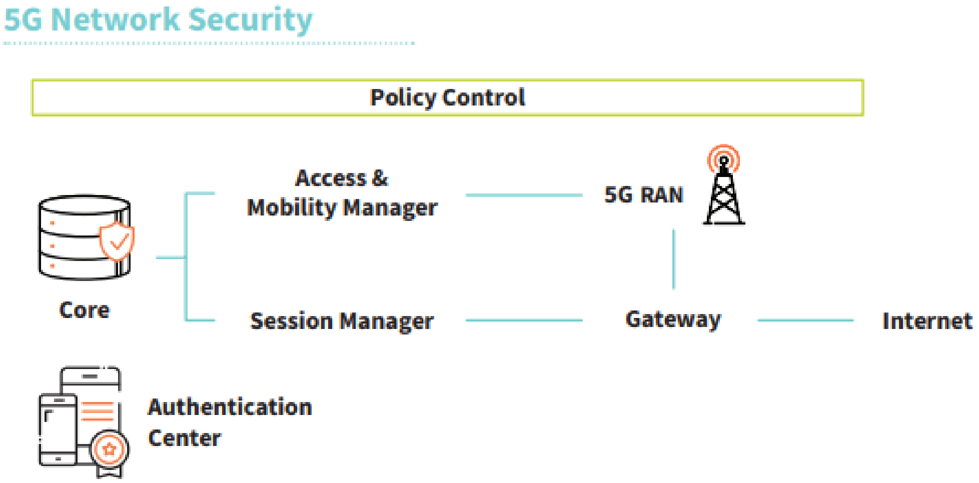
Source: CTIA, PROTECTING AMERICA'S NEXT-GENERATION NETWORKS 10 (2018), https://api.ctia.org/wp-content/uploads/2018/07/ProtectingAmericasNetworks_FINAL.pdf.

Another emerging technology, Virtualized Radio Access Network ("vRAN"), extends network virtualization to the Radio Access Network ("RAN"). The wireless industry is also developing open RAN ("O-RAN"), which combines the attributes of vRAN with open architecture. O-RAN will enable RAN modules from different vendors to interoperate at the same cell site, thus allowing operators to deploy a mix of RAN equipment from various vendors rather than relying on a single vendor per market.

While many factors will determine the evolution and ultimate success of these technologies, the overarching point is that 5G has been designed with a focus on security at the outset. More robust authentication and encryption coupled with network virtualization, edge computing power, device management, and automated threat detection and response will create more flexible and secure networks and contribute to the security of the broader IoT ecosystem.

There are significant architectural differences between 5G and 4G LTE, impacting the RAN, Core, and Edge. "The 5G RAN supports a new larger antenna array known as Massive Multiple Input Multiple Output, and the 5G RAN components are decoupled and distributed. The 5G core network features new configurations, such as network slicing, to support the unique 5G services."[77] Network security features include:

- *Mutual Authentication Functions*. To detect and prevent "spoofing," these functions use an Authentication and Key Agreement protocol between the mobile device and the RAN, allowing the device to authenticate the network, and the network to authenticate the device.
- *IPSec Encryption*. This protocol allows the RAN to encrypt communications between the backhaul connections and the core network and also detect and mitigate unauthorized access, helping ensure proper radio access and prevent denial of service attacks.
- *Access Controls*. These tools enable the detection of unauthorized access to RAN resources and the ability to deny access if appropriate.



Source: CTIA, PROTECTING AMERICA'S NEXT-GENERATION NETWORKS 8 (2018), https://api.ctia.org/wp-content/uploads/2018/07/ProtectingAmericasNetworks_FINAL.pdf.

5G networks will provide increased cybersecurity protections, and commercial providers are taking steps to ensure 5G architecture components mitigate risks.[78] Several innovations in network design and wireless technology will intersect to create highly secure and resilient 5G networks. This results from more agile and layered security as networks transition from

[77] AT&T, 5G POLICY PRIMER: FUTURE WIRELESS NETWORKS WILL HAVE UNPRECEDENTED SECURITY 1 (2018), https://policyforum.att.com/wp-content/uploads/2018/11/5G_Security_1.pdf.

[78] *See* MIKE BURTOK ET. AL., NAT'L CYBERSECURITY CTR. FOR EXCELLENCE, 5G CYBERSECURITY: PREPARING A SECURE EVOLUTION TO 5G (Apr. 2020), https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/5G-pse-project-description-final.pdf.

centralized core and radio access networks to distributed, virtual networks. Architectural improvements, including the Mobile Edge, will provide enhanced security capabilities such as:

- Stronger encryption for over-the-air interface to enhance the security between 5G mobile devices and the 5G network.
- Roaming or network-to-network protection using 5G's new Security Edge Protection Proxy ("SEPP") element at the operators roaming border, which will help mitigate against signaling attacks (e.g., SS7, Diameter) when subscribers are roaming between different carriers' networks.
- 5G Subscriber Identity Privacy using a Subscription Concealed Identifier ("SUCI") to conceal and protect the 5G Subscription Permanent Identifier ("SUPI"), which should help mitigate vulnerabilities to international mobile subscriber identity ("IMSI") catchers.
- Increased Home Network Control for Authentication for the 5G home network to verify that the mobile device is present and requesting service from the serving network.
- 5G Unified Authentication Framework to facilitate use of the same authentication methods for both 3GPP (cellular) and non-3GPP (e.g., Wi-Fi) access networks.
- 5G Security Anchor Function ("SEAF") to facilitate re-authentication of the mobile device when it moves between different access networks or serving networks without having to run the full authentication.[79]

It is not just the network architecture that will enable greater security for 5G. Notable device security enhancements have already been added. These security capabilities are enhancing the IoT overall. Notable developments include:

- *SIM Cards*. An integrated circuit for securely storing and authenticating critical subscriber identity information, a Subscriber Identification Module ("SIM") card enables a secure and reliable voice and data connection and the ability to provision new applications and services remotely.
- *Temporary Identities*. To mitigate the risk of serial numbers being compromised, networks use temporary identities that vary regularly, helping prevent interception by unauthorized users.
- *Wireless Account Controls*. To protect against unauthorized use, consumers can leverage PINs and passwords to protect wireless provider account information, multi-factor account controls to provide more complex user authentication, and text or

[79] AT&T, 5G POLICY PRIMER: FUTURE WIRELESS NETWORKS WILL HAVE UNPRECEDENTED SECURITY 1 (2018), https://policyforum.att.com/wp-content/uploads/2018/11/5G_Security_1.pdf.

email notifications regarding changes in account profiles or number porting requests.

- *Roots-of-Trust*. Built into mobile devices, this hardware-based cryptographic information is used to detect malware and authenticate system software integrity.
- *Anti-Theft Tools*. The mobile industry's voluntary anti-theft commitment provides consumers the tools to locate, lock, and wipe their device in the event of theft or loss.
- *Integrated Systems*. Mobile devices will be able to leverage 5G's advanced authentication and encryption algorithms to work in near real-time with network security enhancements.[80]

With 5G, providers will have the ability to use "advanced authentication systems to better identify the different devices—smartphones, sensors, kitchen appliances, etc.—and tailor security updates to different devices types. This is known as providing native support for plug-in security. 5G's low latency and fast speeds will allow providers to push these customized security updates quickly, with little to no disruption to [users'] service."[81] A further improvement will be better matching of updates to the software needs of specific technology. Device-specific updates will make devices better able to fend off cyber threats and to run more efficiently.

Even with network and device-enabled security features, 5G security requires a layered approach to risk management. The global wireless ecosystem is diverse, extending beyond IT to include OEMs, platform providers, Operating System ("OS") providers, service providers, over-the-top providers, and application developers. Each of these participants needs to prioritize security to have an impact on the overall ecosystem.

In addition, consumers have a role in ensuring a secure communications system, and education is key. For example, consumers should complete various security updates and patching in a timely manner. The federal government can assist with promoting broader consumer and

[80] CTIA, PROTECTING AMERICA'S NEXT-GENERATION NETWORKS 5 (2018), https://api.ctia.org/wp-content/uploads/2018/07/ProtectingAmericasNetworks_FINAL.pdf.

[81] *See What's New in 5G Security? A Brief Explainer*, CTIA (June 12, 2019), https://www.ctia.org/news/whats-new-in-5g-security-a-brief-explainer.

small business education, through efforts already underway.

B. The 5G Ecosystem is Collaborating With Government, Providing a Foundation of Public-Private Partnerships That Should be a Core Principle for 5G Security.

The President's *National Strategy to Secure 5G* committed to "continue to work aggressively with the private sector" on 5G, and the *Request for Comments* asks about stakeholder-driven approaches.[82] Numerous, robust public-private partnerships are aimed at securing 5G networks. These partnerships have been the bedrock of federal cybersecurity policy and are driving supply chain and other efforts in 5G.

While many federal agencies have roles to play, DHS is critical in convening industry and government to work toward common frameworks to address security. DHS's CISA was created by Congress to build on prior effective activities in DHS. CISA promotes public-private partnerships and is constantly working to improve these efforts. In 2018, CISA established the ICT Supply Chain Risk Management Task Force. CTIA and its members actively participate in the Task Force, recognizing that "[e]ffective management of ICT supply chain risks is a national imperative. The scale of this challenge requires a whole of government and whole of society approach" and will help address developments in 5G mobile communications.[83] The Task Force's September 2019 Interim Report describes the work of the Task Force and its working groups and outlines a plan for continued collaboration between the government and key operators in the private sector.[84] The Acting General Counsel of DHS recently commented about

[82] STRATEGY at 2.

[83] *See* CYBERSECURITY AND INFO. SEC. AGENCY, INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE: INTERIM REPORT 1 (2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

[84] *See Id.*

the importance of public-private partnerships.

> Partnership with the private sector is key to so much of the work we do at DHS. We rely on companies to participate in our information sharing forums, including CISA's [ICT] Supply Chain Risk Management (SCRM) Task Force. The ICT SCRM Task Force is a public-private supply chain risk management partnership that includes 20 federal partners – including DoD, which has been a key partner in this and many other DHS initiatives – and 40 of the largest companies in the IT and communications sectors, such as Microsoft, Verizon, Comcast and Cisco. In addition to assembling an inventory of existing supply chain risk management efforts across government and industry, the Task Force has launched four main work streams: developing a common framework for the bi-directional sharing of supply chain risk information between government and industry; identifying processes and criteria for threat-based evaluation of ICT supplies, products, and services; identifying market segments and evaluation criteria for Qualified Bidder and Manufacturer Lists; and, producing policy recommendations to incentivize the purchase of ICT from original manufacturers or authorized resellers.[85]

DHS's NRMC performed a risk assessment for 5G, stating that "5G is expected to bring security improvements and a better user experience, but supply chain, deployment, network security, and competition and choice vulnerabilities may affect the security and resilience of 5G networks."[86] DHS further found that "[t]he effectiveness of 5G's security enhancements will in part depend on proper implementation and configuration,"[87] which is primarily in the hands of industry operators. DHS underscores the importance of promoting a key element of 5G success: interoperability. DHS explained that a "lack of interoperability may also have negative impacts on the competitive market as companies could be driven out if the available competitive market

[85] Chad Mizelle, Acting General Counsel, *Keynote Remarks* (Jun. 17, 2020) https://www.dhs.gov/news/2020/06/17/jones-day-and-berkeley-research-group-s-cyber-supply-chain-and-cmmc-event.

[86] *Overview of Risks Introduced by 5G Adoption in the United States*, CYBERSECURITY AND INFO. SEC. AGENCY (Feb. 3, 2020) https://www.cisa.gov/publication/overview-risks-introduced-5g-adoption-united-states.

[87] CYBERSECURITY AND INFO. SEC. AGENCY, OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED STATES 10 (2019), https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.

decreases."[88]

In its 5G risk assessment, DHS found that the U.S. government can help manage vulnerabilities and increase the security of 5G networks by:

- Encouraging continued development of trusted 5G technologies, services, and products;
- Encouraging continued trusted development of future generations of communications technologies;
- Promoting international standards and processes that are open, transparent, consensus–driven, and that do not place trusted companies at a disadvantage;
- Limiting the adoption of 5G equipment with known or suspected vulnerabilities;
- Continued engagement with the private sector on risk identification and mitigation; and
- Ensuring robust security capabilities for 5G applications and services.[89]

These initial recommendations serve as a strong basis upon which security can be addressed within the 5G ecosystem.

CTIA and its members also actively participate in the FCC's CSRIC. CSRIC Working Groups have examined numerous security issues and 5G development. These reports should be key inputs for NTIA, including its recently completed supply chain risk assessment[90] and CSRIC VII *Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation*.[91] In the latter Report, CSRIC Working Group 2 ("WG2") explores managing security risk in the transition to 5G and examines the risk to 5G from legacy vulnerabilities. WG2 then recommends best practices for mitigation. In December 2020, another *Report on Recommended Updates to*

[88] *Id.* at 11.

[89] *Id.* at 1.

[90] *See* CSRIC WORKING GROUP 3: REPORT ON BEST PRACTICES AND RECOMMENDATIONS TO MITIGATE SECURITY RISKS TO EMERGING 5G WIRELESS NETWORKS (Sept. 2018).

[91] *See* CSRIC WORKING GROUP 2: MANAGING SECURITY RISK IN THE TRANSITION TO 5G, REPORT ON RISKS TO 5G FROM LEGACY VULNERABILITIES AND BEST PRACTICES FOR MITIGATION (June 2020). https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii.

3GPP Standards and Comparison Risk and Remediation Expenses for 5G Vulnerabilities is expected. NTIA should look to CSRIC to assist with implementation efforts.

ATIS is another organization that is working to create 5G-focused supply chain standards and guidelines in consultation with the government. ATIS's 5G Supply Chain Working Group convenes at the request of DoD in consultation with other government agencies. The goal is to extend the development of 5G best practices and guidelines for the purpose of creating supply chain standards that can be operationalized in the public and private sectors.[92] Among other things, the Working Group is focused on establishing "a common assurance framework for trusted 5G networks; develop[ing] or identify[ing] standards to be applied to 5G systems; and evaluat[ing] audit/certification options for ICT solution providers, infrastructure and endpoint device original equipment manufacturers."[93]

In addition to closely engaging with DHS, the FCC through CSRIC, and DoD through ATIS, CTIA and its members are working with NIST and NCCoE on 5G security,[94] including the NCCoE project *Preparing a Secure Evolution to 5G*, which is aimed at showing "how the components of 5G architectures can securely mitigate risks and meet industry sectors' compliance requirements for several 5G use case scenarios."[95] The proposed proof-of-concept solution will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to showcase 5G's robust security features.[96]

Implementation of the *National Strategy to Secure 5G* should leverage these and other

[92] ATIS, *5G SUPPLY CHAIN WORKING GROUP*, https://www.atis.org/01_strat_init/5g-supply-chain/.

[93] *Id.*

[94] *See Preparing a Secure Evolution to 5G*, NAT'L CYBERSECURITY CTR. OF EXCELLENCE, https://www.nccoe.nist.gov/projects/building-blocks/5g-secure-evolution (last visited June 19, 2020).

[95] *Id.*

[96] *See Id.*

efforts, building upon developed relationships and public-private sector collaboration.

C. The Government Should Recognize that Network Responses Should be Dynamic Since Security Challenges and Threats Evolve Over Time.

Wireless network operators face an array of security challenges that try to exploit our interconnectedness and openness, from Distributed Denial of Service ("DDoS") attacks to malware targeting customers. Cyber threats continue to grow, both in number and sophistication. The threats are serious, often launched by highly resourced intelligence services abroad, organized criminal networks, and entities seeking to disrupt domestic and global communications networks. "The United States relies on ICT infrastructure for the functioning of Government, as well as critical services such as banking, utilities, healthcare, and transportation. The pervasiveness of internet protocol-based networks provides a complex attack surface that malicious actors and U.S. adversaries know they can exploit."[97]

As 5G becomes more pervasive, the U.S. government should recognize the innovations that enable the private sector to nimbly address evolving threats and ensure that the *Strategy's* Implementation Plan preserves and promotes flexibility. The telecommunications sector dynamically adjusts its approaches as threats evolve and security mitigations are developed.

Historically, network designers used perimeter defenses to attempt to secure data and functions inside a system, focusing on the core network and the RAN. With 5G, and as network design and security thinking have matured, mobile operators are virtualizing networks, storing functions and elements in the cloud. Innovations in network design and wireless technology will intersect to create a secure and resilient 5G network. Networks will have more agile and layered security as they transition from centralized core and RANs to distributed, virtual networks.

[97] Letter from Ms. Renée James, NSTAC Chair, to the President, at 2 (Apr. 2, 2019) ("NSTAC Letter"), https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem.pdf.

Innovations like network virtualization, edge computing power, device management, and automated threat detection and response will create more flexible and secure networks. Wireless providers are deploying network components that are virtual instead of relying on the hardware. As network functions are virtualized, through NFV and SDN, 5G's virtual and cloud-based network systems will allow for more adaptable security since they can be quickly adjusted, removed, or replaced using software, reducing the likelihood that an entire network would be impacted by a cyberattack.

> Using a broad network of servers to remotely and virtually store data instead of systems of physical hardware increases the wireless network's flexibility, reliability, and security. 5G's speeds, capacity, and near real-time responsiveness will further boost the agility of a virtual network, meaning that more data-intensive applications can be moved to the cloud. Network virtualization will reduce the risk of outages while enabling customized security functions and software-based security updates and tools that can be deployed quickly. Limiting the amount of physical hardware needed to run the network and dispersing network functions to multiple locations also removes targets for a cyber attack.[98]

Within 3GPP, SA3 is a security working group that implements an iterative process to adapt to new security challenges.[99] As challenges and mitigations are developing, 3GPP has adjusted and revised its standards. 5G standards—and security mitigations—are not static.

As critical functions migrate to the edge, mobile network operators are implementing new and embedded security functionalities to ensure a highly secure mobile network. Taking all these innovations and security measures together, the next phase of wireless connectivity will enable enhanced security.

[98] *What's New in 5G Security? A Brief Explainer*, CTIA (June 12, 2019), https://www.ctia.org/news/whats-new-in-5g-security-a-brief-explainer.

[99] *See SA3-Security*, 3GPP, https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security (last visited June 19, 2020).

D. Implementation of the Strategy Should Focus on Harmonizing Ongoing Security Efforts.

One underdeveloped area in the *National Strategy to Secure 5G* is the harmonization of existing federal work on 5G security. There are many fragmented efforts underway, so NTIA should encourage harmonization to avoid conflicting or overlapping work.

The federal government has launched an array of efforts to try to secure 5G networks, some of which are revealing complications, and could benefit from centralized leadership. These include, among several others:

- The Department of Commerce[100] as directed in the 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain[101] proposed ICT supply chain security rules, which are reportedly undergoing review and revisions;
- In 2019, Commerce's Bureau of Industry and Security ("BIS") announced that it was adding Huawei to its Entity List.[102] In May 2020, BIS also published an interim Foreign Direct Product Rule, with additional export controls to prohibit exports, reexports, and transfers of certain foreign-produced items;[103]

[100] *See* Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7), https://www.federalregister.gov/documents/2019/11/27/2019-25554/securing-the-information-and-communications-technology-and-services-supply-chain.

[101] *See* Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 17, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[102] *See* Addition of Entities to the Entity List, 84 Fed. Reg. 22961 (May 21, 2019) (to be codified at 15 C.F.R. pt. 744), https://www.bis.doc.gov/index.php/documents/regulations-docs/2394-huawei-and-affiliates-entity-list-rule/file.

[103] *See* Export Administration Regulations: Amendments to General Prohibition Three and the Entity List, 85 Fed. Reg. 29849 (May 19, 2020) (to be codified at 15 C.F.R. pts. 730, 732, 736, and 744), https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct; *see also* Michael R. Pompeo, *The United States Protects National Security and the Integrity of 5G Networks*, U.S. DEP'T OF STATE (May 15, 2020), https://www.state.gov/the-united-states-protects-national-security-and-the-integrity-of-5g-networks/.

- As noted, DHS has already conducted a substantive risk assessment of 5G implementation, with several recommendations that the federal government could adopt;[104]

- DoD, NASA, and the General Services Administration ("GSA") have a controversial ongoing rulemaking effort to implement prohibitions of Section 889 of the 2019 National Defense Authorization Act ("NDAA"), which would prohibit "the Federal Government from procuring or obtaining, or extending or renewing a contract to procure or obtain, 'any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.'"[105]

- DoD, through the National Spectrum Consortium, issued multiple RPPs for testing 5G applications used in the context of military bases;[106]

- The FCC has barred use of the Universal Service Fund to purchase equipment and services from companies that pose a national security threat.[107]

- The FCC announced 5G test beds, which are "Innovation Zones [that are] city-scale test beds for advanced wireless communications and network research, including 5G networks;"[108] and

- The Secure and Trusted Communications Networks Act of 2019, directed NTIA to establish a program to share information regarding supply chain security risks with trusted providers of communications equipment or services. On June 12, 2020, NTIA issued a notice and request for comments on *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers* to inform the development of the program.[109]

[104] *See Overview of Risks Introduced by 5G Adoption in the United States*, CYBERSECURITY AND INFO. SEC. AGENCY (Feb. 3, 2020) https://www.cisa.gov/publication/overview-risks-introduced-5g-adoption-united-states.

[105] *GSA Guidance on Section 889 FAR Rule*, ACQUISITION.GOV, https://www.acquisition.gov/gsa-deviation/supply-chain-aug13 (last visited June 19, 2020).

[106] *See Current and Upcoming Projects*, NAT'L SPECTRUM CONSORTIUM, https://www.nationalspectrumconsortium.org/project-awards/upcoming-projects/ (last visited June 19, 2020).

[107] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423 (14) (Nov. 26, 2019) https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0.

[108] *FCC Establishes First Two Innovation Zones*, FED. COMMC'NS COMM'N (Sept. 16, 2019), https://docs.fcc.gov/public/attachments/DOC-359737A1.pdf.

[109] *See* Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers, 85 Fed. Reg. 35919 (June 12, 2020), https://www.federalregister.gov/documents/2020/06/12/2020-12780/promoting-the-sharing-of-supply-chain-security-risk-information-between-government-and.

Each of the foregoing has challenges and complexities. These are just a few of the many 5G activities underway at the federal level. NTIA should establish a roadmap for greater coordination between and among these many workstreams.

E. In Implementing the *National Strategy to Secure 5G*, the Government Should Avoid Burdensome Regulation and Mandates.

Security is not static, making prescriptive mandates ill advised. The *National Strategy to Secure 5G* prudently did not call for regulatory solutions. In implementing the *Strategy*, the government should discourage static requirements, which hamstring market participants into compliance mindsets. The 5G ecosystem is quickly developing, and as threats evolve, so will solutions and mitigations, underscoring why it is essential to maintain flexibility—and to promote best practices, but not prescribe hard set solutions.

CTIA urges policymakers to continue collaborating with the wireless industry on important and complex 5G security issues in order to encourage actions that can be taken in standards groups and other organizations. As 5G is deployed, flexibility is critical to meeting the challenge of protecting our networks and consumers against the dynamic global threat landscape.

V. INDUSTRY AND GOVERNMENT CAN MANAGE RISKS TO U.S. ECONOMIC AND NATIONAL SECURITY IN THE GLOBAL DEPLOYMENT OF 5G INFRASTRUCTURE (LINE OF EFFORT THREE).

Under Line of Effort Three, the *Request for Comments* asks about risks to the U.S. economic and national security during development and deployment of 5G infrastructure globally.[110]

[110] *See Request for Comments* at 32017.

A. Global Deployment of 5G Presents Enormous Opportunities for the United States, so Any "Risks Presented by the Use of 5G Worldwide" Need to be Put into Context and Managed, Including with More Proactive Information Sharing by the Government.

The United States dominated 4G LTE deployment and reaped the rewards. The United States has an opportunity to lead and grow its economy by leading the global deployment of advanced telecommunications systems in 5G and beyond.

Carriers, managed service providers, manufacturers, and developers all have opportunities to supply equipment and services overseas, including to parts of the world that are not yet 5G-ready. Global interoperability will foster more innovation. American creators and innovators will benefit when even more of the world is connected, because domestic technology sectors will be poised to provide the services, content, and technology that will be available in some communities for the first time. The U.S. should take actions to support domestic businesses—from fintech to healthcare to entertainment, blockchain, drones, and beyond—that want to offer innovative services around the world.

The *Request for Comments* assumes substantial risk from the use of 5G worldwide. Nevertheless, NTIA should not overlook the economic benefits and security enhancements that will arise from broad 5G deployment and network innovations. To the extent the *Request for Comments* is concerned about global supply chain risks, the origin of manufacturers and software suppliers, and the possibility that untrusted foreign companies may acquire, monopolize, or misuse important emerging technologies, activity is underway to address perceived risks. These activities include, among others:

- The White House Executive Order on ICT Supply Chain security, which creates an entirely new regulatory regime. The rulemaking put forward a view of risk from foreign adversaries, but raised some concerns about its breadth.[111]

- The DHS ICT Task force and the Federal Acquisition Supply Council ("FASC"), which can recommend that certain telecommunications equipment be excluded from federal procurements on national security grounds, are hard at work on these issues.
- NIST offers supply chain risk management approaches and tools.[112]

The government has been aggressive in identifying malicious actors in a variety of actions:

- BIS has imposed severe restrictions on dealings with certain companies.[113] It continues to extend the Temporary General License ("TGL") while asking for input on a more sustainable solution.[114]
- Congress has addressed certain companies in the NDAA.[115]
- The Committee on Foreign Investment in the United States ("CFIUS") and Team Telecom have been reformed and their missions expanded, to review certain transactions.[116]
- BIS is looking at applying export controls to emerging technologies,[117] which should be done with care and sufficient industry input to avoid unintended outcomes.

A key challenge for industry is the multiplicity of actions and workstreams, and the lack of insight into the intelligence and concerns on the part of the government. It is imperative that the government find ways to communicate real concerns to the United States business

[111] *See* Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7), https://www.federalregister.gov/documents/2019/11/27/2019-25554/securing-the-information-and-communications-technology-and-services-supply-chain.

[112] *See, e.g., Draft NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM)*, NAT'L INST. OF STANDARDS AND TECH. (Mar. 2020), https://csrc.nist.gov/publications/detail/nistir/8286/draft.

[113] *See U.S. Department of Commerce Extends Huawei Temporary General License*, DEPARTMENT OF COMMERCE (Nov. 18, 2019), https://www.commerce.gov/news/press-releases/2019/11/us-department-commerce-extends-huawei-temporary-general-license.

[114] *See Department of Commerce Issues Expected Final 90-Day Extension of Temporary General License Authorizations*, DEP'T OF COMMERCE (May 15, 2020), https://www.commerce.gov/news/press-releases/2020/05/department-commerce-issues-expected-final-90-day-extension-temporary.

[115] *See* 2019 NDAA, Pub. L. No. 115-232, 132 Stat. 1636 (2018).

[116] *See* Exec. Order 13913, 85 Fed. Reg. 19643 (Apr. 4, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-establishing-committee-assessment-foreign-participation-united-states-telecommunications-services-sector/.

[117] *See* Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58201 (Nov. 19, 2018) (to be codified at 15 C.F.R. pt. 744), https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

community and innovation base and streamline the sheer number of ongoing efforts. A lack of information about security and geopolitical concerns hampers global business planning and the global rollout of 5G, which cannot be based on conjecture and speculation about what companies or countries are of concern. A coordinated strategy at the federal level is critical.

Numerous commenters in several proceedings have urged the government to rethink its approach to sharing classified information, and to consider ways to communicate concerns about companies *before* investments are made. To that end, CTIA is encouraged by NTIA's recently released request for comments on *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, which seeks feedback to establish a program to share supply chain security risk information with trusted providers of advanced communications service and suppliers of communications equipment or services.[118] This welcomed step must be cohesively implemented with sufficient input from industry, and harmonized with the many workstreams already underway.

B. The *National Strategy to Secure 5G* Should Support Vendor Diversity and Market Competition.

Numerous groups, including the President's NSTAC, cautioned that the diversity of suppliers in the 5G context presents an industry-wide challenge that will require creative government action and private-sector collaboration.

CTIA shares NSTAC's "[c]oncern over supply chain security and resiliency for [national security and emergency preparedness]-critical technologies," which the NSTAC described as the result of a "decreasing diversity of trusted companies that produce certain ICT, for example,

[118] *See* Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers, 85 Fed. Reg. 35919 (June 12, 2020), https://www.federalregister.gov/documents/2020/06/12/2020-12780/promoting-the-sharing-of-supply-chain-security-risk-information-between-government-and.

certain fifth generation (5G) components."[119] The government knows well the importance of having multiple trusted suppliers.

The NSTAC has voiced "concerns about the growing presence of Chinese telecommunications equipment manufacturers, particularly in networks outside of the United States, and the long-term implications for 5G and the broader communications and Internet technology supply chain. This concern is particularly acute in the RAN portion of the network where there are a limited number of RAN equipment suppliers."[120]

One solution may be "driving the industry toward a more interoperable, modular network design that will foster competition between suppliers and lower barriers to entry for new entrants in the marketplace."[121] "As networks have evolved toward software-defined networking (SDN) and network function virtualization, these developments may provide an option to address supply chain concerns" and lower entry costs.[122]

The U.S. government can support industry actions that increase vendor diversity throughout the 5G supply chain. "The Government can undertake initiatives that support the adoption of U.S. technologies across both the private and public sectors. Policymakers can also encourage different sectors of the U.S. government to sponsor the use of new wireless technologies that build on successfully deployed 5G networks. Policies should be developed to provide significant incentives for European RAN vendors to move their R&D resources/facilities to the United States and to develop solutions for the U.S. market."[123]

[119] NSTAC REPORT at 1.

[120] *Id.*

[121] *Id.*

[122] *Id.*

[123] *Id.* at A-14.

Government officials must think strategically and long term. "[T]he United States needs to put in place the right policy framework to support these developments."[124] Short-term policies, recommended by the NSTAC, include acting to:

- *Promote Vendor Diversity.* Persuade allied governments to reduce or eliminate dependency on single-supplier equipment, provide incentives for open RAN R&D, encourage start-ups in o-RAN development, and promote formation of an equipment consortium to promote more open and secure 5G network design.
- *Encourage Open Standards in RANs and Enhanced Interoperability.* Consider O-RAN platforms and carrier adoption of such technologies with real incentives to carriers to deploy multi-vendor, interoperable solutions.
- *Foster Participation in Standards Setting.* Provide tax incentives and other encouragement for participation by U.S. companies and academics in the 3GPP, ATIS, and other relevant standards bodies. Create opportunities for policy makers to gain expertise in and increase support for global standards developments.
- *Incentivize the Adoption of Trusted Technology.* Government can develop incentives for the adoption and use of trusted technology by the public and private sectors.
- *Expedite 5G Deployment and Collaboration.* Eliminate barriers to wireless deployment by supporting both small cell and macro facility upgrades and deployment and making more spectrum available for licensed, exclusive commercial use.
- *Manage an Overall Government 5G Strategy.* Identify a government entity responsible to manage an overall government 5G strategy with cross-sector engagement.[125]

The NSTAC also recognized that the government needs longer-term policies, including:

- *Vital Economic Incentives.* Create vital economic incentives to help drive change by looking at existing tax policy, including tax credits, as incentives for private sector innovations in the 5G ecosystem, R&D, and standards activity.
- *Incentivize Industry Action.* Support long-term industry strategic planning around supply chain resiliency, and provide significant incentives to European and Western O-RAN vendors to move their R&D resources and facilities to the United States and to develop solutions to the U.S. market.
- *Strengthen Expertise and Innovation.* Grant scholarships and other educational incentives to Americans to study wireless technologies, software engineering and cybersecurity in the wireless space, and retain wireless and cybersecurity experts to participate directly or through academic institutions in open software forums.

[124] *Id.* at 6 (emphasis added).

[125] *Id.* at A-3.

Encourage U.S. entities to promote wireless innovations for post-5G developments.

- *Protect Intellectual Property ("IP") and Use Import Controls.* Advocate for aggressive protection of U.S. technology IP rights and use import controls as necessary to support the availability of domestic sources for a diverse 5G supply chain.[126]

C. The United States Should Further Incentivize Investment in 5G Infrastructure and R&D, Use Creative Financing, and Leverage International Cooperation With Like-Minded Partners to Remain Competitive.

The United States government needs to *think bigger* to address the massive differential in R&D spending between Western economies and China.

China pours unparalleled funds into domestic telecommunications R&D and has made certain companies national champions. This gives them an advantage in pricing, market access, and even misappropriation of underlying technologies. Based on its R&D and subsidizing critical industry, China has become a competitor in fast growing high-tech sectors, including 5G. "Looking forward, China's five-year economic plan specifies $400 billion in 5G-related investment."[127] To be sure, simple numerical comparisons will always tend to overstate China's relative progress simply given the substantial population differential between the two countries, a factor that has not precluded U.S. dominance in 4G LTE and related technologies. Yet the means by which China seeks to compete must be taken into account.

Concerns about this are not new. As NSTAC observed, "a primary concern is the growing presence of subsidized competition from China. If Chinese manufacturers continue to gain market share, there is growing concern about the long-term viability of the existing supply chain for 5G and successor technologies. The consolidation of vendors has decreased vendor

[126] *Id.*

[127] DELOITTE, 5G: THE CHANCE TO LEAD FOR A DECADE 1 (2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf.

diversity and created challenges for new entrants. Upfront costs related to labor, equipment, and R&D all work to discourage new communications vendors from competing with established players."[128] "This concern is particularly acute in the RAN portion of the network where there are a limited number of RAN equipment suppliers."[129]

The NSTAC was optimistic that "there are opportunities to correct this in the future,"[130] but the United States government must act swiftly and aggressively. The United States needs a sense of urgency to tackle this disparity with creativity, funding, and commitments to work with like-minded partners.

Solutions will not be easy or complete, but the United States needs to think big, globally, and more strategically to promote a diverse and secure 5G ecosystem. As Senator Rubio has said, "the U.S. cannot escape or avoid decisions about industrial policy."[131] Instead of emulating China's tactics, the U.S. should encourage private sector innovation and collaboration.

Several proposals might shift the imbalance in nationwide investments and should be explored:

- The United States can reconsider tax policy, including tax credits, as incentives for private sector innovations in the 5G ecosystem and standards activity. As a recent Information Technology and Innovation Foundation ("ITIF") paper said, "Congress should make companies' expenditures on global standards setting eligible for the R&D credit. Business investments to participate in global standard-setting processes, including 5G, are an important component to ensuring U.S. competitiveness. But because of the free-rider problem (wherein companies benefit from the actions of

[128] NSTAC REPORT at 6.

[129] *Id.*

[130] *Id.*

[131] MARCO RUBIO, U.S. SENATE COMM. ON SMALL BUS. AND ENTREPRENEURSHIP, MADE IN CHINA 2025 AND THE FUTURE OF AMERICAN INDUSTRY 11 (2019), https://www.rubio.senate.gov/public/_cache/files/d1c6db46-1a68-481a-b96e-356c8100f1b7/3EDECA923DB439A8E884C6229A4C6003.02.12.19-final-sbc-project-mic2025-report.pdf.

other companies), U.S. companies appear to underinvest in standards-settings activities, just as they do in R&D."[132]

- The United States can remove barriers to R&D and partnership with government, including personnel exchanges, and procurement and hiring restrictions that may unintentionally impede collaboration. Working with the government often brings substantial regulatory and compliance burdens, which the government may want to examine in order to expedite and streamline projects. The government should resist the urge to layer on additional regulatory burdens for R&D.
- The United States might build a coalition of like-minded nations to pool and leverage economic power to support R&D. Several voices have called for "long-term planning, inclusive of increased research and development (R&D) spending, to plan for and enable future platforms and applications powered over advanced mobile networks."[133]
- The United States might consider establishing a Multilateral Telecom Security Fund, which could make funds available "to support the development and adoption of secure and trusted telecommunications technologies[,]" upon "the Secretary of State reaching an agreement with foreign government partners to participate in the common funding mechanism."[134]
- Policymakers could modernize the Export-Import Bank's ability to fund 5G-relevant R&D. It may be time to examine the authorities and operations of the Export-Import Bank to see how it could support 5G and future telecom innovation around the world, including with respect to products and services that may not satisfy applicable 85% U.S. content requirements.
- Similarly, it may be prudent to encourage the U.S. Development Finance Corporation to extend financing in more countries to promote R&D and the financing of non-Chinese equipment for the build out to 5G.[135]

VI. THE GOVERNMENT SHOULD PROMOTE AMERICAN VALUES AND RESPONSIBLE GLOBAL DEVELOPMENT OF 5G IN STANDARDS BODIES (LINE OF EFFORT FOUR).

Under Line of Effort Four, NTIA seeks comment on responsible global development and

[132] Doug Brake, *A U.S. National Strategy for 5G and Future Wireless Innovation*, INFO. TECH. AND INNOVATION FOUND. (Apr. 27, 2020), https://itif.org/publications/2020/04/27/us-national-strategy-5g-and-future-wireless-innovation.

[133] NICOL TURNER LEE, BROOKINGS, NAVIGATING THE U.S.-CHINA 5G COMPETITION 1 (2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_5g_competition_turner_lee_v2.pdf.

[134] S. 3189 116th Cong. § 2(c) (2020), https://www.warner.senate.gov/public/_cache/files/2/3/2365fc6a-422c-4df2-837b-f297bb293ad2/E8131EF8149D5D0E1411683ABC3DECCD.oll20034.pdf.

[135] *See* Yuko Koshino, *How the US Can Promote Affordable Non-Chinese 5G in Asia*, INT'L INST. FOR STRATEGIC STUDIES (Mar. 20, 2020), https://www.iiss.org/blogs/analysis/2020/03/jc-5g-in-asia.

deployment of 5G, including how the U.S. government can promote, incentivize, and foster greater private sector participation in global standards development.[136]

A. The U.S. Government Should Support Broad Participation in International 5G Standards Bodies but Allow the Private Sector to Lead.

Global technical standards are vital to facilitating the widespread availability and adoption of 5G, including its technical trajectory and core interoperability. There are important ongoing activities at the International Telecommunication Union ("ITU"), 3GPP, ATIS, Internet Engineering Task Force ("IETF"), Institute of Electrical and Electronics Engineers ("IEEE"), and elsewhere. 5G is built on global consensus standards and specifications informed by almost 600 organizations working to meet international expectations for the next generation of interoperable wireless communications.[137]

It is critical to distinguish platforms that are appropriate for direct federal participation (like the ITU) from those in which federal government support should be indirect and as a convener (like 3GPP).

The ITU is a vital venue for global coordination and harmonization of 5G, spectrum, and radio technologies, but is unique in structure and operation, making a direct role for the U.S. government necessary and appropriate. "The ITU, which designates 5G as International Mobile Telecommunication 2020 (IMT-2020), laid out a vision for IMT-2020 in 2015 and has been developing and refining requirements for IMT-2020."[138] IMT-2020 goals address peak data

[136] *See Request for Comments* at 32017.

[137] *See* AT&T, 5G POLICY PRIMER: THE GLOBAL STANDARDS PROCESS IS ROBUST AND EFFECTIVE IN ADVANCING U.S. GOALS (2020), https://policyforum.att.com/wp-content/uploads/2020/03/5G-Standards-Whitepaper-March-2020.pdf.

[138] THE WHITE HOUSE, EMERGING TECHNOLOGIES AND THEIR EXPECTED IMPACT ON NON-FEDERAL SPECTRUM DEMAND 1 (2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/Emerging-Technologies-and-Impact-on-Non-Federal-Spectrum-Demand-Report-May-2019.pdf.

rates, user experience data rates, spectrum efficiency, mobility, latency, connection density, network energy efficiency, and area traffic capacity, all of which are essential aspects of 5G.[139]

The U.S. government directly engages at the ITU by sending a delegation of private sector and federal agency advisors that coordinate with private sector participants. The government plays an important role in the ITU, which is distinct from the private sector-led 3GPP. Given the impact of ITU decisions on treaty-level text, and the involvement of other competing national governments, the role of U.S. government needs to be more engaged in the discussions pertaining to spectrum management and allocations, while leaving the development of IMT specification standards to industry and private sector participants.

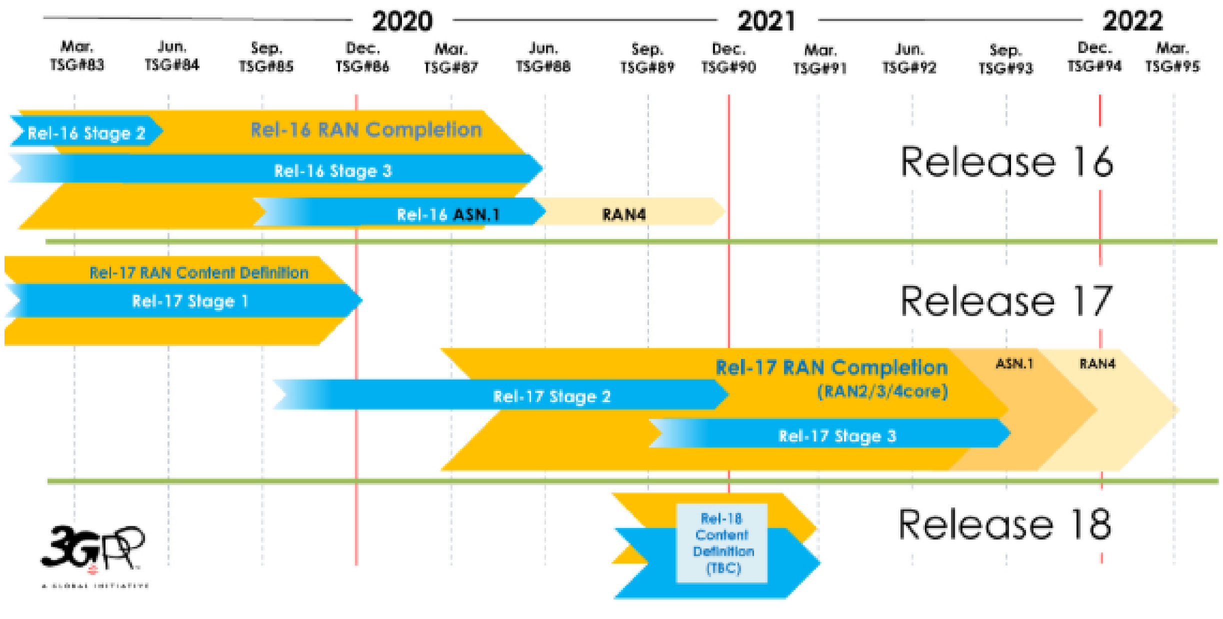
The 3GPP is a key specification-settings body in which 5G is being developed. It is fundamentally different from the ITU. It does not create regulations or treaty obligations or any binding requirements. It creates technical standards that support interoperability of communications networks and transmissions. Wireless technology evolves as features are introduced by 3GPP via Releases. This has been done since 2G. Releases are not rigidly timed, and work is done on multiple Releases simultaneously in phases. Releases are iterative, in that they build upon prior Releases. 3GPP has a dedicated working group for 5G security, SA3, which makes its work public and is tackling key improvements and lessons learned from 4G. 3GPP standards for 5G are already well underway. Release 15 is complete for non-standalone and standalone 5G,[140] and Release 16 is nearing completion.[141] Input for Release 17 is

[139] *Id.* at 9, Figure 2.3.

[140] *See Release 15*, 3GPP (last updated Apr. 26, 2019), https://www.3gpp.org/release-15.

[141] *See Release 16*, 3GPP (last updated Mar. 23, 2020), https://www.3gpp.org/release-16.

ongoing.[142] More 5G system enhancements are set to follow in Release 17.[143] These standards are implemented in new technologies and will enable new features not available with 4G LTE.[144]



Source: 3GPP TSG SA#87e, 17-20 March 2020, e-meeting document SP-200222

© 3GPP 2020

Source: *Releases*, 3GPP, https://www.3gpp.org/specifications/releases (last visited June 19, 2020).

The 5G process has more input than past specifications because operators and manufacturers recognize the importance of contributing to a global standard. Hundreds of companies and organizations participate in 3GPP to vet contributions and develop standards. The process is driven by engineers, which supports technically sound ideas and standards.[145]

3GPP is a global partnership of standards development organizations and operates by consensus among private sector and technology experts. It is not susceptible to one country's

[142] *See Release 17*, 3GPP, https://www.3gpp.org/release-17 (last visited June 19, 2020).

[143] *See Id.*

[144] *See* NSTAC REPORT at A-3.

[145] *See* AT&T, 5G POLICY PRIMER: THE GLOBAL STANDARDS PROCESS IS ROBUST AND EFFECTIVE IN ADVANCING U.S. GOALS 4 (2018), https://policyforum.att.com/wp-content/uploads/2018/10/5G_Policy_Primer_Global_Standards.pdf.

control. Its iterative process relies on hundreds of expert engineers evaluating members' contributions on their technical merit, and they can be discarded or substantially evolve over time. The 3GPP process is transparent, collaborative, and consensus based. No country, region, industry segment, or company can dominate its activities or its outputs.[146] 3GPP procedural rules promote regional balance and transparency. Hundreds of members work through seven Organizational Partners. Work in 3GPP is done in Working Groups that formed under Technical Specification Groups ("TSG"s). Each TSG is led by a Chair and Vice Chairs elected by the members, with term limits and regional diversity requirements. The entire ecosystem is working toward interoperability between networks and devices and economies of scale needed for global development of new technology. Any non-standard deployment will not be scalable or interoperable with other networks.

All of this makes a recent proposal by DoD troubling, as it is potentially disruptive to the 3GPP global standards process and would invite opposition from allies that reasonably object to government efforts to control or influence standards, as well as a disproportionate response from nations with less benign motives. DoD's recently released *5G Strategy* states that "DoD will fully implement its Standards Engagement Plan and will actively participate in the 3rd Generation Partnership Project (3GPP) organization."[147] However, governments do not drive 3GPP standards development, and direct U.S. military involvement could be seen as a heavy-handed insertion into the industry and engineer-led consensus process. This could have the unintended consequence of undermining the technical consensus-based efforts of U.S. companies that have engaged in this process for years. There are other venues for the DoD to engage,

[146] *See id.* at 3.

[147] DEP'T OF DEF., DEPARTMENT OF DEFENSE (DOD) 5G STRATEGY 7 (May 2, 2020), https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf.

including in consultation with other federal agencies before the ITU.

There are additional industry-led efforts, including the IETF, which is developing security requirements for network protocols for end-to-end device security and the IoT. These efforts build on several successful security protocols and standards IETF has developed, such as IP Security, Transport Layer Security, and Simple Authentication and Security Layer.

The American National Standards Institute ("ANSI") works to enhance the global competitiveness of U.S. businesses by promoting and facilitating voluntary consensus standards and ensuring their integrity. Additionally, ANSI promotes the use of United States standards internationally, and advocates American policy and technical positions in international and regional standards organizations, while encouraging the adoption of international standards as national standards where these meet the needs of the user community.[148] ANSI's efforts extend to cybersecurity[149] and 5G standards.[150]

The European Telecommunications Standards Institute ("ETSI") is responsible for the standardization of cybersecurity standards internationally and for providing a center of relevant expertise for information and communications technologies, including mobile. The standards include global encryption technologies and algorithms to support integrity, authentication, and privacy.

GSM Association ("GSMA"), a global trade association, leverages the contributions of its many members around the globe to share best practices and create standards for security management in mobile networks.

[148] *See* ANSI, *Standards Activities Overview* (last visited Jun. 19, 2020) https://www.ansi.org/standards_activities/overview/overview?menuid=3.

[149] *See* ANSI, *Cybersecurity Portal* (last visited Jun. 19, 2020) https://www.ansi.org/cyber/default?menuid=3.

[150] *See* ANSI, *5G Headlines* last visited Jun. 19, 2020) https://www.ansi.org/news_publications/latest_headlines?menuid=7&newsTag=5G&AvailableForAlert=False.

An increased presence by American companies and experts is vital, but the U.S. government should not dictate or try to superintend standards work. Such an approach would validate the perceived misdeeds of other nations and usurp the important central role of private expertise and innovators to develop technical standards by consensus. The global telecommunications ecosystem has a history of collaborating on standards. It is left to private experts—engineers, scientists, and other builders—to debate technical problems and solutions, working toward consensus in a transparent way.

The United States can continue to promote interoperability, openness, and diversity in technology and standards bodies. As previously stated, part of a solution in the short-term may be to drive "toward a more interoperable, modular network design that will foster competition between suppliers and lower barriers to entry for new entrants in the marketplace."[151]

The government can support and encourage participation in global 5G standards-setting bodies, as recommended in the NSTAC report and addressed above by "[p]rovid[ing] tax incentives and other encouragement for expanded participation by U.S. companies and academics in the [3GPP] and other standards bodies."[152]

The government should also "[c]reate opportunities for policy makers to gain expertise in and increase support for global standards developments."[153]

[151] NSTAC REPORT at 6.

[152] *Id.* at A-2.

[153] *Id.*

> Extensive expertise is required to maintain U.S. global technology leadership, participate heavily in global standards development, and implement a shift toward greater diversity and 5G network models and capabilities. Scholarships and other education incentives encouraging more Americans to study wireless technologies, software engineering, and cybersecurity will be key to expanding the U.S. pool of expertise around 5G networks and, with it, the extraordinary capabilities of these new technologies.[154]

The U.S. government "should retain wireless and cybersecurity experts to participate directly or through academic institutions in open software forums. Policymakers should encourage the many relevant components of the U.S. government to promote innovations of new wireless technologies building on successfully deployed 5G networks."[155]

To maintain its leadership, the United States needs commitment by even more organizations to contribute as members, in organizations such as 3GPP and ATIS. Standards development driven by the private sector will ensure robust participation and foster U.S. technological leadership for the next decade and beyond. Importantly, it will also transfer institutional knowledge as longstanding corporate representatives train junior experts to carry forward this important work. This is particularly vital as standards work relies on relationships of trust built on shared expertise and collaboration.[156]

B. A National Strategy Should Support Options Including Open Platforms and Open Source Development Without Picking Winners or Losers.

The United States government can also assist by increasing the availability of R&D funding for next-generation wireless technologies, to foster innovation in open standards and approaches, without dictating solutions for operators or choosing winners or losers in the

[154] *Id.* at A-14.

[155] *Id.*

[156] *See* AT&T, 5G POLICY PRIMER: THE GLOBAL STANDARDS PROCESS IS ROBUST AND EFFECTIVE IN ADVANCING U.S. GOALS 9 (2020), https://policyforum.att.com/wp-content/uploads/2020/03/5G-Standards-Whitepaper-March-2020.pdf.

marketplace.

The government could support R&D for the use of industry-led open standards and enhanced interoperability, such as the standards under development at the O-RAN Alliance, 3GPP, ATIS, IETF, and elsewhere. The government can foster innovation in open standards and approaches, without dictating solutions for individual operators.

As discussed, O-RAN is a promising option, which offers disaggregated functionality built using open interface specifications between elements. The benefits of this type of development are based in vendor-neutral hardware and software-defined technology built through open interfaces and community-developed standards. According to the O-RAN Alliance, this will allow smaller vendors to introduce their own services and allow operators to customize the network as needed. It will also allow multiple vendors to deploy their technology on the network, thereby enabling competition and reducing costs.[157] Open Core has also been getting attention as a way to innovate, including by the Telecom Infra Project.[158] CSRIC VII, WG 2 addressed these, and other ongoing CSRIC workstreams are engaged as well.

Open source development is also an area that could result in greater transparency. The use of open source software by mobile network operators will likely increase and the community will benefit from the expanded use that will result from the addition of companies in the 5G

[157] *See* O-RAN ALLIANCE, O-RAN: TOWARDS AN OPEN AND SMART RAN (2018), https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5bc79b371905f4197055e8c6/1539808057078/O-RAN+WP+FInal+181017.pdf.

[158] *See Open Core Network*, TELECOM INFRA PROJECT, https://telecominfraproject.com/open-core-network/ (last visited June 19, 2020).

ecosystem. As a result, it is likely that the increased visibility into open source software will result in improvements in vulnerability detection, reporting, and patching.[159]

The United States government should engage industry on all of these fronts, as overcoming the current R&D imbalance will require massive investments into promising technologies and platforms.

VII. CONCLUSION.

CTIA and its members are leading the way on 5G security and partnering with myriad government agencies to lead global innovation and deployment. CTIA looks forward to working with NTIA on these vitally important issues and U.S. policy to support a secure 5G future.

/s/ Melanie K. Tiano
Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President, General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John A. Marinho
Vice President, Technology and Cybersecurity

[159] *See Communications Security, Reliability, and Interoperability Council VII*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii (last visited June 19, 2020).