Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

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

COMMENTS OF
CONSUMER TECHNOLOGY ASSOCIATION

Consumer Technology Association ("CTA")®[1] hereby responds to National Telecommunications and Information Administration ("NTIA")'s request for comments to inform development of an implementation plan for the National Strategy to Secure 5G ("Strategy").[2] CTA applauds the Administration for recognizing in the Strategy the critical importance of 5G wireless technologies to our nation's prosperity and security and welcomes the opportunity to provide input on the Strategy's implementation.

The wireless and consumer technology industries are moving rapidly to develop standards for 5G wireless services and roll out 5G products and services in a race to meet consumer demand. 5G is "a game-changer"—the "platform technology for everything from digital health to augmented and virtual reality … enabling internet speeds 100 times faster than

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the largest, most influential tech event on the planet.

[2] *The National Strategy to Secure 5G Implementation Plan*, Notice; Request for Public Comments, Docket No. 200521-0144, RIN 0660-XC047, 85 Fed. Reg. 32016 (May 28, 2020) ("RFC"). The Secure 5G and Beyond Act of 2020, Pub. L. No. 116-129, requires development of a strategy and implementation plan to ensure the security of next generation wireless communications systems and infrastructure.

today's networks."[3] CTA's members are leading this revolution, including major manufacturers of mobile devices, wireless infrastructure manufacturers, network operators, and start-up technologists who view networks as the foundations for their businesses. They design and manufacture the millions of 5G-capable handsets and tablets on the market today and will continue to be central players in the 5G revolution.[4]

As the Covid-19 crisis continues, it requires unprecedented performance from mobile networks, including remote work, health, and schooling capabilities. And, next-generation networks are transforming American lives and industries. Innovation in connectivity is more central to consumers and the U.S. economy than ever before. Thus, the consumer technology industry is highly incentivized to meet consumers' expectations for increasing connectivity and work toward public policy solutions that support this result.

CTA believes that the U.S. government can best facilitate the accelerated development and rollout of 5G infrastructure in the U.S. and lay the groundwork for innovation beyond 5G by continuing to make more spectrum available, reducing unnecessary government barriers, remaining technology-neutral, and supporting and promoting—but not itself running—standards-setting and other voluntary and multistakeholder efforts. To advance security in 5G, the Administration should rely on consensus standards and multistakeholder fora that allow the private, public, and international sectors to collaborate and drive security innovation at scale. Promoting responsible international development and deployment of 5G and the availability of

[3] Jeffrey Hill, CTA's Gary Shapiro: *State, Local Governments Lagging on 5G Adoption*, Via Satellite (Sept. 23, 2019), https://www.satellitetoday.com/government-military/2019/09/23/ctas-gary-shapiro-state-local-governments-lagging-on-5g-adoption (quoting Gary Shapiro).

[4] *See generally* Comments of CTA to FCC, GN Docket No. 20-60 (filed Apr. 27, 2020).

secure and reliable equipment and services is best done by supporting industry-led, open, and voluntary global interoperability standards for communications and information technologies.

I. THE ADMINISTRATION CAN BEST FACILITATE DOMESTIC 5G ROLLOUT WITH COMMERCIAL SPECTRUM, INFRASTRUCTURE REFORM, AND CONSENSUS STANDARDS AND MULTISTAKEHOLDER FORA

Pushing 5G to all Americans on a fast timeline and a broad scale requires more spectrum, faster deployment, and light-touch regulation. Facilitating domestic rollout of 5G technologies and development of a robust domestic 5G commercial ecosystem requires (i) a continued focus on making more spectrum available in mid-, low, and high bands; (ii) reforms of the Federal, state, and local rules governing infrastructure deployment; and (iii) support for the development of voluntary standards and industry multistakeholder processes that further innovation.[5]

Increasing Spectrum Availability and Improving Spectrum Management. The billions of connected devices entering the consumer products market rely on spectrum, and wireless networks will need greatly increased capacity and access to a variety of spectrum bands for both licensed and unlicensed use.[6] America's 5G leadership thus depends on a robust spectrum policy that maximizes the availability of all spectrum bands, and that properly balances reliance on licensed, shared or lightly licensed, and unlicensed spectrum bands. Connected devices, and the consumers who use them, benefit from access to networks that utilize new low-, mid-, and high-band spectrum.[7] Indeed, one of the keys to the game-changing capabilities of 5G is the use of a wide variety of spectrum bands for fixed and mobile applications. Future services will use

[5] *See* RFC at 32,017 (seeking comment on "Line of Effort One: Facilitate Domestic 5G Rollout").

[6] *See* Comments of CTA, NTIA Docket No. 181130999-8999-01, RIN 0660-XC C044 (filed June 8, 2020).

[7] *See* Comments of CTA to FCC, GN Docket No. 14-177, at 5 (Jan. 23, 2017), https://ecfsapi.fcc.gov/file/10123665715360/CTA_Spectrum_Frontiers_2FNPRM_Comments.pdf ("CTA Spectrum Frontiers Comments").

multiple spectrum bands, with the network and devices employing the most appropriate frequencies for delivery of a particular service.[8]

In recent years, the Federal Communications Commission ("FCC") has moved forward in releasing low-, mid-, and high-band spectrum, and unlicensed spectrum, for new 5G services.[9] Even with these actions, consumer demand for increased connectivity, faster speeds, and more data continues to grow. To meet this exponential demand, innovators require sufficient access to spectrum that will support next-generation services. Ensuring continued innovation in new 5G and next-generation products and services requires the federal government to keep the spectrum pipeline flowing and promote policies that support diverse business models and applications.

America's forward-thinking spectrum policy, combined with the introduction of mobile broadband operating systems, made possible the increased connectivity that contributed to "hockey stick growth in many dimensions—device sales, data traffic, apps, advertising, payments, social media, and much more."[10] By making both licensed and unlicensed spectrum available for commercial use in conjunction with other innovation-friendly policies, government set the stage for companies to invest and innovate in the U.S. in new connected products and services.[11] Not only did this investment and innovation benefit consumers in ways previously not imagined, but it also yielded dividends in the form of economic growth and job creation. For

---

[8] *See, e.g.*, News Release, T-Mobile, *T-Mobile, Ericsson and Intel Complete World's First 5G Call on 600 MHz* (Jan. 7, 2019), https://www.t-mobile.com/news/600-mhz-5g-call (At CES 2019, T-Mobile, Ericsson, and Intel demonstrated this future at CES with 5G first—a tri-band 5G video call, where each caller used a different spectrum band: 600 MHz, 28 GHz, and 39 GHz.).

[9] *See, e.g.*, The FCC's 5G FAST Plan (last visited June 10, 2020), https://www.fcc.gov/5G.

[10] CTA, 5G U.S. Market Impact, at 2 (2018), https://shop.cta.tech/products/5g-us-market-impact ("5G Market Impact Study").

[11] *See* CTA, International Innovation Scorecard 2019 – United States (Jan. 3, 2019), https://cdn.cta.tech/cta/media/media/advocacy/scorecard/intl-pdfs/2019-international-innovation-scorecard-web-united-states.pdf ("2019 International Innovation Scorecard").

example, although there were just five companies that had crossed the billion-dollar threshold in 2010, this number ballooned to 120 by 2018—with half of these billion-dollar companies located in the U.S.[12]

America's future global competitiveness depends upon the same type of forward-thinking spectrum policymaking that previously enabled American leadership in wireless broadband connectivity over the past decade. Indeed, the stakes for leading in 5G and other advanced wireless connectivity may be higher than ever: The deployment of 5G technologies likely will occur in concert with other significant technological breakthroughs in artificial intelligence, Internet of Things ("IoT"), robotics, blockchain, user interfaces, and edge computing—all technologies that either rely on, or can be enhanced by, wireless connectivity. With these innovations occurring in conjunction with 5G deployment, there could be three to five times more disruption in the 5G cycle as compared to the 4G cycle.[13] Put in monetary terms, this 5G "value chain" could generate $3.5 trillion in revenue and support 22 million jobs between 2022 and 2035.[14] To ensure America realizes these economic benefits, the federal government must have a plan to ensure commercial access to new spectrum by the current and next generation of connected devices and products.

To meet the growing demand for wireless bandwidth and to ensure that America maintains its global competitiveness, the government also should seek to improve federal spectrum management—specifically, to increase transparency regarding how federal spectrum is used and what federal spectrum could be made available for commercial use. This could include

[12] 5G Market Impact Study at 14.

[13] *Id*.

[14] IHS Economics & IHS Technology, *The 5G economy: How 5G technology will contribute to the global economy*, at 18 (Jan. 2017), https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf.

(i) developing methods for ongoing measurement of federal spectrum use;[15] (ii) providing public results of these measurements, subject to any national security concerns, to allow for engagement on how to best use limited spectrum resources; and (iii) establishing a roadmap identifying bands that are being explored for future commercial use on an exclusive or shared basis.[16] The government should employ every available tool to increase access to spectrum across the board, while accounting for critical federal uses, including: (i) prioritizing efficient use of spectrum by Federal users;[17] (ii) continued collaboration among NTIA, the FCC, and Federal users to maximize sharing opportunities; and (iii) creating a positive environment for research and development ("R&D").[18]

Streamlining Infrastructure Regulations. The federal government should continue its effort to streamline infrastructure siting regulations, which is critical to securing America's 5G leadership. CTA especially commends the FCC's aggressive actions to promote mobile

[15] By some accounts, the federal government occupies—either exclusively or on a primary basis—sixty percent of the spectrum best suited for mobile broadband. *See, e.g.*, FCC Commissioner Michael O'Rielly, *Enacting More "Sticks": Spectrum Fees for Government Users*, FCC Blog (Sept. 8, 2015), https://www.fcc.gov/news-events/blog/2015/09/08/enacting-more-sticks-spectrum-fees-government-users. This measurement should happen on a recurring basis to enable an assessment of whether spectrum is being used efficiently.

[16] CTA previously urged the FCC to issue a roadmap that would describe the timing related to the release of spectrum in the pipeline. Specifically, CTA recommended that such a roadmap include dates, in the near term, for holding spectrum auctions. Similar to an FCC roadmap, providing estimated timing about the Administration's activities to free up spectrum would give the industry and consumers useful information to plan commercial development and deployment of 5G and next generation wireless products and services that would utilize these bands. NTIA also should explore the possibility of a joint FCC/NTIA roadmap that could provide a more comprehensive picture of the timeline for making more spectrum available for commercial use.

[17] For example, the FCC held commercial auctions for the 1695-1710 MHz, 1710-1755 MHz, 1755-1780 MHz, and 2155-2180 MHz bands to commercial users. The majority of the federal systems have been relocated out of these bands. *See* Wilbur Ross & David Redl, U.S. Department of Commerce, *Commercial Spectrum Enhancement Act (CSEA): Annual Progress Report for 2017* (June 2018), https://www.ntia.doc.gov/files/ntia/publications/csea_2017_report_june_2018.pdf.

[18] Investments in research and development create the foundation for the innovation economy. *See* Comments of CTA to NTIA, Docket No. 1603311306-6306-01, RIN 0660-XC024 at 27-28 (June 2, 2016), https://www.ntia.doc.gov/files/ntia/publications/cta_comments_re_ntia_iot_rfc-final-060216_2.pdf. In fact, a country's gross expenditures (regardless of the source of funds) on research and development is one indicator CTA uses to evaluate the extent to which countries are innovation-friendly. *See* CTA, 2019 International Innovation Scorecard, Methodology, https://www.cta.tech/Policy/Innovation-Scorecard/International/Methodology.aspx.

broadband and fixed wireless deployment by reducing the substantial hurdles faced by providers seeking to deploy 5G wireless infrastructure. These advances have spurred new deployment, promising to bring the benefits of ultra-fast mobile broadband, and the devices that rely on it, to American consumers.[19] Despite the significant hurdles cleared and the progress made to date, the FCC should continue its efforts to make efficient infrastructure deployment a priority.

Pursuing Technologically Neutral Policies and Supporting, Not Leading, Standards Efforts. Finally, a light government touch can help ensure that voluntary standards and multistakeholder processes are robust and effective. The government should not pick winners and losers in the 5G marketplace, except in extreme circumstances where dictated by specific and irremediable security concerns. Remaining technology- and business-neutral requires refraining from mandates, allowing for both open RAN and integrated solutions, avoiding government-run interoperability certification programs, and otherwise assuming that government should substitute its judgment for that of companies on the front lines of R&D and consumer demand.

Private sector standards development processes are among the most important vehicles of private sector leadership, as the rigorous vetting and testing of technical approaches in these processes constitute the peer-reviewed technical foundations of 5G deployment. Many of CTA's members participate in the 3rd Generation Partnership Project (3GPP), the venue in which all 5G standards, including security standards, are being developed. The U.S. government should broadly support and promote private sector participation in standards processes, but it should not intervene in or coordinate U.S. industry positions; instead, it should maintain the longstanding practice of looking to industry stakeholders to develop these standards in processes that have

[19] *See* Comments of CTA to FCC, GN Docket No. 19-285 (filed Dec. 9, 2019).

been to date—and we expect will continue to be—open and transparent. CTA cautions policymakers against generalizing the extent to which foreign actors influence 3GPP and its processes. 3GPP is an industry-led body with company voting—not country voting.

II. GOVERNMENT SHOULD WORK WITH INDUSTRY TO ASSESS RISKS TO AND IDENTIFY CORE SECURITY PRINCIPLES OF 5G INFRASTRUCTURE

CTA's technology security efforts have historically focused on technical standards activities pertinent to consumer technology, but in recent years—as consumer technology has itself become more pertinent to broader Information and Communications Technology Services ("ICTS") ecosystem security concerns—CTA has significantly broadened and deepened its security efforts.[20] Thus, CTA's members are very well suited to identify factors that the government should consider in developing core security principles for 5G infrastructure and in evaluating trustworthiness or potential security gaps in 5G infrastructure, including the supply chain.[21]

In recent years, CTA's government engagement promoted security approaches focused on risk management and public-private collaboration. For instance, CTA is an active member of the Sector Coordinating Councils for both the Information Technology and the Communications sectors. These are the vehicles through which industry engages the Department of Homeland Security ("DHS"), Cybersecurity and Infrastructure Security Agency, and its National Risk Management Center, the government's lead institution for analyzing and addressing critical infrastructure security risks pertaining to 5G. In addition, CTA members are active in the

[20] *See* Comments of CTA, NTIA Docket No. 200504-0126, RIN 0660-XC04 (filed June 8, 2020).

[21] *See* RFC at 32,017 (seeking comment on "Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure").

influential work of the FCC's Communications Security, Reliability and Interoperability Council ("CSRIC"), including its working groups on 5G security.[22]

Similarly, this model of government-facilitated industry leadership through partnership and collaboration across government is working to secure the 5G supply chain. For instance:

- The Communications Sector Coordinating Council contributed substantially to the first version of the DHS risk assessment required under Section 5(b) of EO 13873, and industry will continue to do so in the subsequent updates and improvements of this required annual assessment.
- The ICT Supply Chain Risk Management Task Force is a formally chartered industry-government partnership in which both the leadership and the membership of the Task Force is a 2-to-1 industry-to-government ratio. Among several other workstreams with substantive deliverables, Working Group 1 is developing legal and procedural recommendations for a regime to govern the sharing between industry and government of derogatory information or suspicions regarding certain suppliers.
- NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, is the federal government's primary guide to supply chain risk management; like other NIST risk management guidance, this publication both benefits from and promotes private sector expertise and experience.

These are models of private sector leadership and cross-sector collaboration that should be expanded globally.

With respect to addressing particular supply chain risks, CTA supports a precisely targeted and risk-oriented approach with procedural clarity, based on clear definitions.[23] The U.S. government should establish a precisely targeted approach to identify and address threats to the supply chain, based on discerning analysis of specific risks. Focusing the scope of the potentially prohibited transactions and specifying the risks that certain policies or rules seek to

[22] *See, e.g.*, CSRIC VII Working Group 2, *Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation* (June 10, 2020), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii.

[23] *See* Comments of CTA to Department of Commerce, Office of the Secretary, Docket No. 191119-008, RIN 0605-AA51 (filed Jan. 4, 2020).

address will help ensure that such actions have the intended consequences—and avoid negative unintended consequences to this important market.

The looming threat that a transaction might later be unwound retroactively is likely to have a chilling effect on U.S. innovation and technology investment and would create an incentive for companies to move investment offshore to avoid potential U.S. unwinding. In addition, broad prohibitions on transactions may impair U.S. leadership in technical research and standards development—activities that are inherently global.

The government should not impose new restrictions on supply chain transactions exclusively pertaining to: (i) commercially available off-the-shelf consumer items; (ii) technical research and testing for standards and specification development, adoption, and conformance; or (iii) products that are already subject to national security oversight by other agencies or other regulatory regimes. Nor should the government adopt any rules restricting supply chain transactions that do not have a demonstrated nexus to a specific threat or vulnerability identified in the Office of the Director of National Intelligence's or DHS' threat and vulnerability assessments.

Most important, to ensure effective ICTS supply chain security policies, the broad set of U.S. government supply chain security activities must be closely coordinated to ensure they are not in conflict or duplicative.[24] Restrictions in this area are unprecedented and foundational,

[24] *See, e.g.*, the FCC's proceeding on *Protecting Against National Security Threats to the Communications Supply Chain through FCC Programs*, which preliminarily designated Huawei and ZTE as covered entities for which Universal Service Fund support is prohibited; implementation of the National Defense Authorization Act for Fiscal Year 2019 Section 889's prohibitions on federal procurement from Huawei and ZTE, and from entities that "use" Huawei and ZTE; future "exclusion orders" issued by the Federal Acquisition Security Council for federal procurement; the Department of Defense's implementation of its Cybersecurity Maturity Model Certification program for defense contractors; the ICT Supply Chain Risk Management Task Force, particularly the working group focusing on developing legal and procedural mechanisms for sharing of derogatory information on specific suspect suppliers; and nascent processes at NTIA and elsewhere on software supply chain security and transparency (*e.g.*, developing a "software bill of materials").

and, as such, will have profound long-term impacts both globally and within related or parallel U.S. policy activities.

III. THE GOVERNMENT SHOULD ADDRESS WORLDWIDE 5G INFRASTRUCTURE DEPLOYMENT RISKS TO U.S. ECONOMIC AND NATIONAL SECURITY BY RELYING ON INDUSTRY AND DIPLOMACY

CTA's members are poised to seize the opportunities for U.S. companies in the 5G ecosystem, recognizing that doing so depends on successfully addressing the risks—both real and imagined—of 5G.[25] The best path to address the risks to national security is to continue to rely on consensus standards and multistakeholder fora that allow the private, public, and international body sectors to collaborate.[26] CTA co-leads, with USTelecom, one such example of a multistakeholder forum, the Council to Secure the Digital Economy ("CSDE"), a group of more than a dozen major ICTS companies deeply invested in the security of our communications infrastructure and connected products ecosystem.[27] CSDE has convened important discussions and produced tools to aid companies and governments alike.

In November 2018, CSDE released the International Anti-Botnet Guide ("Guide").[28] The Guide is a playbook that offers companies across the digital ecosystem a set of baseline tools, practices and processes they can adopt to help protect against the threat of botnets and other automated, distributed attacks. The Guide provides a flexible approach for IoT devices of

---

[25] RFC at 32017 ("Line of Effort Three: Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide."); *see also* Mark Lynas, *Anti-Vaxxers and Russia Behind Viral 5G COVID Conspiracy Theory*, Cornell Alliance for Science (Apr. 8, 2020), https://allianceforscience.cornell.edu/blog/2020/04/anti-vaxxers-and-russia-behind-viral-5g-covid-conspiracy-theory/.

[26] *See generally* Comments of CTA, NTIA Docket No. 200504-0126, RIN 0660-XC04 (filed June 8, 2020).

[27] *See* Council to Secure the Digital Economy, Member Companies, https://securingdigitaleconomy.org/member-profiles (last visited June 2, 2020).

[28] *See* CSDE, *International Botnet and IoT Security Guide 2018*, https://www.ustelecom.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf.

varying processing capabilities and data types, providing companies with a range of options to appropriately address security risks. This past November, CSDE released updates to the Guide for 2020.[29]

In 2019, through CSDE, CTA convened 20 major cybersecurity and technology organizations, industry associations, consortia, and standards bodies—all groups that convene their own security-focused memberships. This unprecedented industry effort, known as "Convene the Conveners" or "C2," sought to identify baseline security capabilities for the rapidly growing IoT marketplace to address four challenges:

- Promoting global harmonization to prevent fragmentation of security specifications and requirements.
- Working with emerging global market forces that naturally favor secure devices and systems.
- Developing a coherent common language on these issues that is compelling to various policy and technical audiences.
- Assisting policy development internationally and in the United States, including at the state level.

The first product of this effort was released on September 17, 2019.[30] Through this effort and other avenues, CTA and many of its member companies have collaborated closely with leaders at NIST—in particular, assisting NIST in its thoughtful approach to developing a "Core Baseline for IoT Devices" recently finalized in NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline*[31]—as well as with NTIA, DHS, and other government agencies.

---

[29] CSDE, *International Botnet and IoT Security Guide 2020*, https://securingdigitaleconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf.

[30] CSDE, *The C2 Consensus on IoT Device Security Baseline Capabilities*, https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

[31] Michael Fagan et al., *NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline* (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf; *see also* Michael Fagan et al., *NISTIR 8259,*

The government's efforts in developing the Roadmap Toward Resilience Against Botnets and the work that has followed also represent how a multistakeholder process can achieve results. CSDE worked closely with the Departments of Commerce and Homeland Security in their development of *A Roadmap Toward Resilience Against Botnets*.[32] The development of the C2 Consensus is one outcome of that multistakeholder process.

CTA also convened a working group of cybersecurity experts to draft a voluntary industry consensus standard for IoT baseline security.[33] This document (draft CTA-2088) is in the final stages of approval and publication and is anticipated by manufacturers, retailers, and other stakeholders as an important element of the drive to secure the IoT. CSDE's success in creating the Guide, C2 Consensus, and its recent work with the Departments of Commerce and Homeland Security represent the strengths of a multistakeholder process. The multistakeholder process is bearing fruit in the United States and it will continue working globally.

The RFC also seeks comment on any incentives/policy options to close or narrow security gaps and ensure the economic viability of the domestic industrial base.[34] As CTA stated in comments to the U.S. Trade Representative ("USTR"), tariffs put some CTA members—particularly innovative startups—at a disadvantage relative to their competitors in other

---

Foundational Cybersecurity Activities for IoT Device Manufacturers (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

[32] *See, e.g.*, U.S. Department of Homeland Security & U.S. Department of Commerce, *A Roadmap Toward Resilience Against Botnets* (Nov. 29, 2018), https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_1.pdf (noting that CSDE will be a contributor for numerous tasks described in the Road Map).

[33] *See generally* CTA, Status of Active Consumer Technology Association Projects, https://standards.cta.tech/kwspub/current_projects (noting that CTA's R14 Cybersecurity and Privacy Management Committee WG1 is working to turn the Guide's language of best practices into technical standard language) (last visited June 2, 2020).

[34] RFC at 32,017 ("What incentives and other policy options may best close or narrow any security gaps and ensure the economic viability of the United States domestic industrial base, including research and development in critical technologies and workforce development in 5G and beyond?").

nations.[35] They fear that those competitors will be able to undercut them in the market by continuing to import critical components from China, now at a fraction of the cost to U.S. businesses. Other startups fear that the tariffs, and the resulting business and economic uncertainty, will prevent their products from going to market entirely.

American companies doing business in China often face limitations, including ambiguous and ever-changing regulations and a lack of clarity in Chinese law, many of which USTR specifically addressed in its Report on the Section 301 Investigation. But actions taken to address inequity in the trade relationship with China should not include tariffs that harm our competitive advantage over foreign companies. Tariffs are an indirect and blunt tool that saddle U.S. companies and consumers with added costs. Many companies that were already engaged in efforts to combat Chinese patent infringers and counterfeiters—for instance by keeping higher paying intellectual property ("IP"), research, design and engineering jobs in the U.S.—cannot afford the added burden of tariffs as high as 25%. And Chinese retaliation on U.S.-origin products has further compounded the burden U.S. companies face financially.

A better approach is to promote and encourage innovation and technological progress here in the United States. Appropriate laws, regulations, and deregulation at both the state and federal levels have and will continue to help U.S. companies strengthen their comparative advantage in technological innovation vis-à-vis China and the rest of the world.

CTA welcomed the constructive dialogue in which the Administration and Chinese officials engaged to reach a "phase 1" tariff deal. CTA further encourages multilateral

[35] Comments of CTA, USTR Docket No. USTR-2018-0005 (filed May 11, 2018); *see also* Comments of CTA, USTR Docket No. USTR-2019-0015 (filed Sept. 20, 2019).

diplomatic engagement with China, allowing nations also injured by China's unfair trade practices to leverage a collective counterbalancing strength.

Key priorities for these efforts should include: (i) clarification and increased transparency in Chinese IP laws; (ii) continued implementation of China's specialized and unified IP court system; encouragement of innovation with progressive rather than protectionist laws; (iii) increased legal and regulatory due process; increased fines for IP violations; and (iv) increased enforcement activities, including joint or plurilateral programs. CTA has a rich history of working with our member companies on U.S. patent reform, and with sister organizations in foreign jurisdictions on similar issues. Modernizing China's patent system would not only create a fairer trade environment, it would also save our innovative companies years of lost production and significant costs on litigation.

The U.S. should use the WTO platform to engage our trading partners in the fight for fair trade rules with China leveraging the strengths of others to help attain broader concessions from China than perhaps the U.S. could achieve unilaterally. Continuing to negotiate and enter into strategic multi- and plurilateral trade agreements will also aid U.S. competitiveness. CTA stands willing to help in such multilateral efforts.

IV. PROMOTING RESPONSIBLE GLOBAL DEVELOPMENT AND DEPLOYMENT OF 5G STARTS WITH SUPPORTING INDUSTRY-LED, OPEN, AND VOLUNTARY GLOBAL INTEROPERABILITY STANDARDS

The government can best lead responsible international development and deployment of 5G and promote availability of secure and reliable equipment and services by supporting industry-led, open, and voluntary global interoperability standards for communications and information technologies.[36] This approach will ensure security needs are met while also

[36] RFC at 32017 ("Line of Effort Four: Promote Responsible Global Development and Deployment of 5G").

maximizing innovation. As noted in a separate NTIA docket, CTA supports the NTIA's proposal "to advocate for standards from [Standards Developing Organizations ("SDOs")] developed using a consensus-based, industry-driven approach; that industry should lead international standards development processes, and that those processes should be transparent and open."[37]

As in other areas of telecommunications, consensus-based technical standards and interoperability in 5G are most likely to reflect the most current technological developments and practical solutions available. For instance, many CTA members are engaged in promoting open and interoperable standards for Radio Access Networks and other aspects of advanced telecommunications networks through initiatives such as the O-RAN Alliance, the Open RAN Policy Coalition, and the Telecom Infra Project. The consumer technology marketplace is both innovative and competitive in the United States and worldwide. The current voluntary global standards process reflects this competitive environment by promoting innovation and flexibility while providing for interoperability and security.

A wide range of industry-led multistakeholder SDOs and industry consortia are already leading the development of telecommunications and information standards with respect to artificial intelligence/machine learning, consumer protection, cybersecurity, digital economy, IoT, healthcare tech, and unmanned aerial vehicles. Standards and specification development for these emerging technologies are best left to the organizations already working in these areas such

[37] Comments of CTA, NTIA Docket No. 200504-0126, RIN 0660-XC04 (filed June 8, 2020); *see Request for Comments on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly*, Docket No. 200504-0126, RIN 0660-XC04, 85 Fed. Reg. 27,390, 27,390 (May 8, 2020).

as ISO ("International Organization for Standardization"), International Electrotechnical Commission ("IEC"), regional groups (*e.g.* ETSI) and industry groups (*e.g.* IEEE and CTA).[38]

CTA commends the U.S. government for globally advocating for the deployment of trusted and secure 5G equipment. While CTA does not take a position for or against U.S. government financial support for industry, we do agree that it is in the U.S. national interest to support trusted and secure 5G equipment. Certain policies help. For example, the U.S. International Development Finance Corporation ("DFC," previously the Overseas Private Investment Corporation) has been supporting the deployment of trusted and secure 5G network equipment. Where statutory barriers exist with regard to potential partnerships in middle- and upper-income countries, Congress could remove such barriers.[39] Similarly, the U.S. Export-Import Bank ("EXIM") has also recognized the need to support trusted suppliers with competitive export financing. Given the diverse content of all trusted suppliers' 5G equipment, EXIM should adopt a more flexible approach to U.S. content rules. Such an approach might include taking into account U.S. R&D and IP as well as significantly lowering U.S. content

[38] *See* ISO, About Us, https://www.iso.org/about-us.html ("ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies."); International Electrotechnical Commission, About the IEC, https://www.iec.ch/about/?ref=menu ("The International Electrotechnical Commission (IEC) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic, and related technologies. Close to 20,000 experts from industry, commerce, government, test and research labs, academia, and consumer groups participate in IEC Standardization work."); Institute of Electrical and Electronics Engineers, About IEEE, http://www.ieee.org/about/index.html ("IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. IEEE and its members inspire a global community to innovate for a better tomorrow through its more than 419,000 members in over 160 countries, and its highly-cited publications, conferences, technology standards, and professional and educational activities."). CTA has an extensive Technology and Standards program that includes more than 70 committees, subcommittees, and working groups; roughly 1,100 participants; and holds American National Standards Institute ("ANSI") accreditation.

[39] Congress has recognized a need for an exemption for energy projects and similarly should enact one to support global deployment of secure and trusted telecommunications infrastructure. The European Energy Security and Diversification Act of 2019, P.L. 116-94, Div. P, Title XX, eases DFC's less-developed country requirement for energy infrastructure projects in Europe and Eurasia. This authority for energy projects, which provides commercial opportunities in upper-middle-income countries that may have both strategic and development benefits, should be extended globally for deployment of secure and trusted telecommunications infrastructure.

requirements to support the national security priority to finance deployment of secure and trusted telecommunications infrastructure.[40]

It is important to note, as suggested in the RFC,[41] that the issues raised in this proceeding are inherently intertwined with the Department of Commerce's ICTS supply chain proceeding and with the recent Bureau of Industry and Security ("BIS") proceeding to clarify the effect of Entity List actions and associated export control requirements on participation in standards and industry consortia processes.[42] In these proceedings, government agencies have proposed or undertaken actions that would adversely impact U.S. leadership in R&D, standards setting, testing, and more. While perhaps not intended, these restrictions will have the effect of impairing the United States' lead in 5G and other next-generation technologies, particularly in the development of global, harmonized interface specifications. For example, BIS recently added more companies to the Entity List and seems poised to continue to do so; as more companies are added, there are in some cases unintended consequences that actually can harm U.S. interests and penalize companies not on the Entity List.[43]

For instance, participation in standards and specifications development bodies include IP rights obligations. If a company with a strong IP position is blocked from participating in such bodies, they will not be subject to the IP rights obligations (e.g., to license their IP on reasonable

---

[40] *See, e.g.*, Export-Import Bank of the United States, Short-term content policy, https://www.exim.gov/policies/content/short-term-content-policy (last visited June 25, 2020); *Id.*, Medium and long-term content policy, https://www.exim.gov/policies/content/medium-and-long-term (last visited June 25, 2020).

[41] RFC at 32,017 (seeking comment on "Line of Effort Four: Promote Responsible Global Development and Deployment of 5G" as well as the questions "Both the Department of Commerce and the Federal Communications Commission (FCC) have rulemakings underway to address the security of the telecommunications infrastructure supply chain. Are there other models that identify and manage risks that might be valuable to consider?") (footnote omitted).

[42] *See* Bureau of Industry and Security, *Release of "Technology" to Certain Entities on the Entity List in the Context of Standards Organizations*, Interim final rule; request for comments, 85 Fed. Reg. 36,719 (June 18, 2020).

[43] Bureau of Industry and Security, *Addition of Entities to the Entity List, Revision of Certain Entries on the Entity List*, Final rule, 85 Fed. Reg. 34,495 (June 5, 2020).

and non-discriminatory terms) that are associated with participation—but these very obligations help protect other companies involved in the standards process and those seeking to adopt and implement the standard.

Essential patents in wireless communications can also come from outside the 5G process. All major SDOs support Reasonable and Non-Discriminatory ("RAND") IP requirements for participation, so the current uniformity in patent protections in all areas benefits all equally. If there are different restrictions on participation in 5G standards- and specifications-setting bodies versus non-5G bodies, protection for U.S. companies (including carriers, device makers, chip makers, and software makers) will be compromised. The U.S. government should take great care not to upset the apple cart of a functional standards development process that has been carefully refined over more than a century of standards setting and intellectual property rights law development.

Finally, CTA notes that the U.S. government should tread carefully in terms of Department of Defense ("DOD") engagement in standards processes.[44] Of course, it is not unreasonable for DOD as a customer of technology with the highest-level security needs to seek to ensure that its requirements will be met. However, in terms of global leadership and innovation, the Administration should consider whether U.S. government, and specifically DOD, involvement in standards setting would send the wrong message—including whether it would give cover for military institutions from other countries to seek to engage in 5G standards and

[44] Justin Doubleday, Defense Dept. Looks to Participate in Global 5G Standards-Setting Bodies, Inside Defense (June 8, 2020) ("The Pentagon has established a new 'tiger team' to engage fifth-generation wireless standards bodies … 'We don't typically get engaged in standards, but because of this 5G being so important to the department we found it necessary to engage the standards bodies, the [3rd Generation Partnership Project], the ATIS. … We're in partnership with industry, the federal government, and others, not just from a U.S. perspective, but from a global perspective.'") (quoting Frederick Moorefield, Jr., deputy chief information officer for command, control, and communications).

whether it would suggest that the intelligence community may be seeking inroads into 5G standards development processes.

V. CONCLUSION

As NTIA develops the U.S. government's plan to secure 5G, CTA urges the government to prioritize actions that support industry, such as freeing up spectrum for commercial use, reducing unnecessary government barriers to innovation, implementing technology-neutral policies, and supporting voluntary, industry-led standards. Consensus standards and multistakeholder fora that allow the private, public, and international body sectors to collaborate can best identify and address national security risks. In addition, the Administration should continue to engage internationally to promote deployment of trusted and secure 5G equipment. CTA welcomes the continued opportunity to assist the Administration in implementing the Strategy and advancing American leadership on 5G.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Jamie Susskind*

Jamie Susskind
Vice President, Policy and Regulatory Affairs

/s/ Mike Bergman
Mike Bergman
Vice President, Technology and Standards

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

June 25, 2020