Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

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

COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION
(CompTIA)

Dileep Srihari
Vice President and Senior Policy Counsel

Savannah Schaefer
Senior Director, Public Advocacy

COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION
322 4th Street NE
Washington, DC 20002

June 25, 2020

TABLE OF CONTENTS

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

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

COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION
(CompTIA)

The Computing Technology Industry Association ("CompTIA"),[1] the leading association for the global information technology (IT) industry, respectfully submits these comments to the National Telecommunications and Information Administration ("NTIA") in response to the above-captioned Request for Comments ("RFC").[2]

INTRODUCTION AND SUMMARY

The importance of 5G and communications infrastructure has never been more apparent. The COVID-19 pandemic with the massive economic and physical dislocations it has caused have illustrated how much the United States depends on communications networks for both economic and national security. Recognizing the importance of that security, CompTIA supported enactment of the Secure 5G and Beyond Act of 2020 ("Act") in March and we appreciated the Administration's prompt issuance of the National Strategy to Secure 5G

[1] CompTIA supports policies that enable the information technology industry to thrive in the global marketplace. We work to promote investment and innovation, market access, robust cybersecurity solutions, commonsense privacy policies, streamlined procurement, and a skilled IT workforce. Visit www.comptia.org/advocacy to learn more.

[2] NTIA, *The National Strategy to Secure 5G Implementation Plan*, RIN 0660-XC047, 85 Fed. Reg. 32016 (May 28, 2020) ("RFC").

("National Strategy") required by the Act.[3] We welcome this opportunity to comment on the National Strategy's four Lines of Effort and on the Implementation Plan being developed pursuant to Section 4 of the Act.

The Administration is right to consider a holistic approach to national and economic issues related to 5G development and deployment. As described below, the ecosystem for wireless technologies is changing rapidly. Competition in established markets for wireless network equipment and services is increasing, and current global trends toward open architectures and virtualization will likely increase such competition in the years ahead, ultimately benefitting the United States. The pace of global innovation in wireless technology also continues to increase, and the government must therefore adopt a forward-looking approach to national and economic security that considers not just 5G in its initial form, but also future wireless technologies.

The most immediate objective for the government should be to continue aggressively facilitating domestic rollout of 5G technologies (**Line of Effort One**). The Administration and Congress should forge a new national consensus to end the diversion of spectrum auction revenue to non-telecommunications purposes, instead reinvesting such revenue into broadband deployment, better federal spectrum management, and a "research dividend" for wireless research and development ("R&D"). Congress and the Administration should also enact legislation to streamline broadband infrastructure siting and promote workforce training to address a significant shortage related to broadband deployment.

[3] Pub. L. No. 116-129, 134 Stat. 223 (Mar. 23, 2020); President Donald J. Trump, *National Strategy to Secure 5G of the United States of America* (Mar. 2020), *available at* https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf

Next, security is foundational to the successful deployment of 5G. As the government works to assess risks to and identify core security principles of 5G infrastructure (**Line of Effort Two**), it should begin by leveraging the new security features that are incorporated into 5G, using them to inform decisions. The government should continue relying on whole-of-government, risk-based approaches than enhance the ICT ecosystem's ability to manage and communicate risks across a variety of disparate stakeholders and sectors of the economy. It should double-down on key public-private partnership efforts, leverage private-sector leadership via technical standards, and collaborate more deeply with other like-minded nations, including by supporting crucial work at the State Department like the Prague Proposals.

The National Strategy also calls for addressing risks to U.S. economic and national security during development and deployment of 5G infrastructure worldwide (**Line of Effort Three**), but identifies just two specific goals: management of supply chain risks in U.S. government infrastructure and addressing the threat of "high-risk" vendors in U.S. 5G infrastructure. Congress and the Administration have already taken several steps in that regard, although in some cases the work needs refinement. But the RFC appropriately goes further, as 5G deployment also brings significant opportunities to advance U.S. economic and national security. The government should pro-actively encourage industry trends toward open radio access network ("RAN") architectures and software-based networking technologies that will ultimately favor the United States.

The Administration wisely focuses the National Strategy on promoting responsible global development and deployment of 5G (**Line of Effort Four**), although the work should consider future wireless technologies as well. Building on the State Department's work on global 5G supply chain security issues via the Prague Proposals, the federal government should establish a

Multilateral Telecom Security Fund, as envisioned in recent legislation introduced in Congress. It should also revise the U.S. International Development Finance Corporation rules to support strategic investments in 5G technologies in Europe and Eurasia, revise the U.S. Export-Import ("EXIM") Bank rules to support trusted suppliers, and expand the federal R&D tax credit to encompass participation in standards development activities while avoiding politicization of the standards process.

Finally, although these comments are structured to follow the Lines of Effort described in the National Strategy, many of the RFC questions and specific details in the Strategy could apply to multiple "Lines of Effort." For that reason, many of the specific proposals below are readily transferable to, or should be duplicated in, other portions of the Implementation Plan.

DISCUSSION

I. THE ECOSYSTEM FOR WIRELESS TECHNOLOGY IS CHANGING RAPIDLY.

The Secure 5G and Beyond Act and the National Strategy to Secure 5G that resulted from it each reflect a concern by the federal government that the United States risks being left behind in the global race to 5G development and deployment. While some segments of the market do reflect concentration, the story of 5G networks and technology is actually a much broader one wherein the United States leads across many of the elements essential to 5G networks, as explained below. Meanwhile, policymakers across party lines and agencies are focused on addressing the immediate challenge regarding national security risks that may be posed by equipment from certain vendors. However, policymakers must begin to view 5G development and deployment against the backdrop of wider changes that are happening in the global wireless technology ecosystem.

A. Competition in 5G Technology is Broader Than Commonly Understood and the United States is a Leader in Emerging Trends.

The traditional elements of a network used to be more well-defined – routers, switches, wireless base stations, etc. However, these elements – including the specific elements necessary for radio access networks ("RANs") – are now often aggregated, partitioned, or virtualized. For example, a traditional radio base station is now often partitioned into a separate baseband unit ("BBU") that generates a digital radio frequency ("RF") signal, and a remote radio head ("RRH") that sends and receives analog signals and connects to the antenna. Meanwhile, as 5G networks are designed to provide not just high-bandwidth but also low-latency services, some network functions that were previously handled in the core are increasingly being pushed closer to the edge. As the government assesses the state of 5G, its future direction, and the implications for economic and national security, it must take a holistic view of 5G that considers all of these elements.

RAN hardware. Much attention over the last several years has focused on the idea that there are just five companies providing 5G RAN infrastructure – Huawei, ZTE, Nokia, Ericsson, and Samsung. While those companies are indeed leaders, others are emerging to compete in 5G radio access networking products. For example, the Japanese company NEC is actively being considered by the United Kingdom as a potential alternative to Huawei and the company is seeking 5G business in other countries as well.[4] Meanwhile, many technologies underlying 5G radio networks have been developed by U.S. companies like Intel and Qualcomm, and will

[4] *See, e.g.*, Kitty Donaldson, Tim Ross, and Thomas Seal, *U.K. Opens Talks With Huawei Rival as Johnson Confronts China*, BLOOMBERG, June 3, 2020, https://www.bloomberg.com/news/articles/2020-06-03/u-k-opens-talks-with-huawei-rival-as-johnson-confronts-china; Tom McIlroy, *NEC Pitches Itself as Huawei Replacement in 5G Rollout*, FINANCIAL REVIEW, June 22, 2020, https://www.afr.com/politics/federal/nec-pitches-itself-as-huawei-replacement-in-5g-rollout-20200621-p554mo.

incorporate advances in semiconductors from those companies. Indeed, these and other American companies sell components to all of the major 5G RAN infrastructure manufacturers. Thus, even as policymakers may be focused on RAN infrastructure vendors, the U.S. continues to enjoy a strong position of overall leadership on the technologies underlying 5G.

Emerging trends. The 5G ecosystem depends not just on radio access technology, but also on core and edge networking technologies where there are a variety of U.S. players such as ADTRAN, Cisco, Juniper, and Oracle – many of whom also compete directly with Huawei and ZTE for 5G-related business.[5] Meanwhile, Wi-Fi 6 is built upon many of the same technologies underlying 5G, and the U.S. enjoys a strong position of leadership in Wi-Fi.[6] At present, Wi-Fi and 4G LTE routinely complement each other, and future 5G and industrial and enterprise environments will take this significantly further. Advanced 5G will offer the possibility of selecting between, or combining connectivity through, multiple different radios managed by both mobile network operators and enterprise private networks. Over time, mobile 5G networks and private networks combining 5G and Wi-Fi may begin to converge, and the line between the RAN

---

[5] *See, e.g.*, Press Release, *ADTRAN Delivers Fixed Wireless Access Solutions to Accelerate 5G Deployments*, Feb. 26, 2019, https://www.adtran.com/index.php/adtran-delivers-fixed-wireless-access-solutions-to-accelerate-5g-deployments; Will Townsend, *Cisco Systems Goes Big on 5G*, FORBES, Feb. 27, 2020, https://www.forbes.com/sites/moorinsights/2020/02/27/cisco-systems-goes-big-on-5g/#4a3574638fe7; Juniper Networks, *5G Networks*, https://www.juniper.net/us/en/solutions/5g-networking/ (visited June 18, 2020); Oracle, *Oracle Communications 5G Next Generation Core*, https://www.oracle.com/industries/communications/service-providers-network/solutions/5g-next-generation-core/ (visited June 23, 2020).

[6] *See generally* Cisco, *5 Things to Know About Wi-Fi 6 and 5G*, https://www.cisco.com/c/m/en_us/solutions/enterprise-networks/802-11ax-solution/nb-06-5-things-WiFi6-5G-infograph-cte-en.html (visited June 24, 2020); Intel, *5G vs. Wi-Fi 6: A Powerful Combination for Wireless*, https://www.intel.com/content/www/us/en/wireless-network/5g-technology/5g-vs-wifi.html (visited June 24, 2020); Lee Doyle, *When to Use 5G, When to Use Wi-Fi 6*, NETWORK WORLD, June 12, 2019, https://www.networkworld.com/article/3402316/when-to-use-5g-when-to-use-wi-fi-6.html.

and other edge-based network elements may begin to blur further, with U.S. companies playing an ever-greater role.

Even regarding the 5G RAN itself, emerging trends point toward Open RAN architectures that permit disaggregation of RAN components using common interfaces, facilitating greater competition. In addition, virtualized RAN – that is, RAN infrastructure built using commodity hardware and silicon that runs specialized software – will likely begin to emerge. As described further in section IV-A below, these trends will favor the United States over the long term, and any policy geared toward enhancing U.S. national and economic security surrounding 5G should account for them.

B. New "Generations" Will Appear More Rapidly, Necessitating Long-Term Policy Planning to Support the Ecosystem.

Although enhancing U.S. competitiveness in 5G is important, the federal government's focus must also consider the long term. In the past, "generational" changes in commercial mobile radio technology were perceived to occur roughly every ten years, but there is no evidence that this pattern will continue in the future. To the contrary, the 3GPP standards body already updates its releases on a more frequent basis, incorporating many new features along the way. For example, 4G LTE was first introduced in with 3GPP Release 8 in 2008, but was eventually supplemented with LTE-Advanced in Release 10 (2011), carrier aggregation in Release 12 (2015), and LTE-U / LAA in Release 13 (2016). 5G elements were first introduced in Release 14 (2017), with the 5G Phase 1 specification in Release 15 (2018).[7] While the inclusion of the 5G Phase 2 specification in this year's forthcoming Release 16 will be an

[7] Electronics Notes, *3GPP Specification Release Numbers*, https://www.electronics-notes.com/articles/connectivity/3gpp/standards-releases.php (visited June 18, 2020).

important landmark, it is still only a benchmark "for an *initial* full 3GPP 5G system."[8] Further evolution and improvements will doubtless follow in the years to come.

Meanwhile, trends toward Open RAN architectures will potentially make equipment upgrades easier to accomplish, since different components using a common interface could potentially be swapped separately without needing to replace an entire system. This trend would likely make technology upgrades for carriers both cheaper and more frequent, reflecting incremental rather than generational improvements over time. In addition, virtualized RAN and other network function virtualization ("NFV") that are implemented in software that runs on commodity hardware may also make some upgrades faster and easier, in some cases potentially without any hardware modifications. (*See also* section IV-A below.)

Policy implications. The government should therefore not focus its attention simply on whether a particular carrier operating in the United States or an allied nation is using equipment from a particular hardware vendor. While there may be specific security challenges in specific subsegments of the 5G infrastructure marketplace, the government should instead focus most of its attention on supporting a strong technology ecosystem to ensure that the nation remains a leader not just in cellular "5G," but in all of the wireless technologies that will follow and surround it (including Wi-Fi) – whether labeled with a "G" or not.

II. LINE OF EFFORT ONE: FACILITATE DOMESTIC 5G ROLLOUT.

United States leadership in 4G deployment benefited Americans tremendously. One estimate indicated that U.S. 4G leadership meant roughly $125 billion in revenue to American companies that could have gone elsewhere if the United States had not led on 4G, without even

[8] 3GPP, *Release 16*, https://www.3gpp.org/release-16 (visited June 18, 2020).

accounting for indirect effects.[9] Ensuring the same level of success for 5G is therefore an important national priority. Thus, the federal government must step up its efforts to promote both 5G deployment and the development of future wireless technologies, including complete reinvestment of spectrum auction revenue, more efficient federal spectrum management, investment in research and development, streamlined infrastructure siting policies, and broadband infrastructure workforce development.

A. End Diversion of Spectrum Auction Proceeds for Non-Telecommunications Purposes.

In recent decades, the federal government has obtained tens of billions of dollars in auction proceeds for spectrum licenses, but a relatively small amount is reinvested into the telecommunications sector. Instead, Congress has used spectrum auction proceeds to pay for unrelated spending or tax cuts.[10] For example, the AWS-3 auction that concluded in 2015 yielded total bids exceeding $44 billion, of which approximately $30 billion was eventually allocated to the Treasury for unrelated purposes.[11] The 600 MHz band incentive auction yielded

[9] Recon Analytics, *How America's 4G Leadership Propelled the U.S. Economy*, at 1 (Apr. 16, 2018), *available at* https://api.ctia.org/wp-content/uploads/2018/04/Recon-Analytics_How-Americas-4G-Leadership-Propelled-US-Economy_2018.pdf.

[10] Section 6413 of the Middle Class Tax Relief and Job Creation Act of 2012 allocated at least $20.4 billion and ultimately much more to deficit reduction. Pub. L. No. 112-96 §§ 6413(b)(5), (b)(8), 126 Stat. 156, 235-36 ("2012 Spectrum Act"). The Spectrum Pipeline Act of 2015, which was included in the Bipartisan Budget Act of 2015, was estimated to raise $5 billion over 10 years, nearly all of which was used to offset other non-communications costs. Pub. L. No. 114-74, Title X, 129 Stat. 584, 621-25; CBO, *Estimate of the Budgetary Effects of H.R. 1314, the Bipartisan Budget Act of 2015, as reported by the House Committee on Rules on October 27, 2015*, at 4, Oct. 28, 2015, https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/costestimate/hr1314.pdf.

[11] From $44 billion in bids, NTIA estimated total relocation costs of approximately $5 billion and the 2012 Spectrum Act allocated $7.55 billion for specific telecommunications purposes including FirstNet, *see* 2012 Spectrum Act § 6413(b), leaving roughly $30 billion for the Treasury.

total bids of nearly $20 billion, of which over $7 billion went to unrelated deficit reduction, and the upcoming C-Band auction is likely to yield at least $15 billion in additional net revenue for the Treasury.[12] Meanwhile, some in Congress are now considering spending $80 billion to move the nation close to universal connectivity.[13] Indeed, if all spectrum auction proceeds in the past two decades had simply been re-invested into broadband deployment, *the country would likely have achieved universal access to broadband by now*. The re-investment would also have strengthened the overall U.S. technology ecosystem, improving the sector's ability to promote economic and national security.

While the past cannot be changed, the United States now faces a moment when its leadership in technology is being challenged by other countries just as broadband access is more essential than ever. Policymakers can therefore no longer afford to treat spectrum auction revenue as a national piggy bank to be raided whenever the occasion demands. The Administration and Congress should instead work together to forge a new national consensus to eliminate spectrum auction fee diversion for any purpose beyond the ICT sector. All funds should instead be re-invested into areas including broadband deployment, better spectrum management, core wireless technology research, and other communications-related purposes.

---

[12] *See, e.g.*, Grant Gross, *Giant FCC Spectrum Auction Raises $19.8 Billion, Sets Up 5G Services*, NETWORKWORLD, Apr. 13, 2017, https://www.networkworld.com/article/3190029/giant-fcc-spectrum-auction-raises-198-billion-sets-up-5g-services.html (Treasury to receive $7.3 billion from 600 MHz auction); Congressional Budget Office, *Cost Estimate for S. 2881, 5G Spectrum Act of 2019*, at 3 (Feb. 24, 2020), https://www.cbo.gov/system/files/2020-02/s2881.pdf (estimating net offsetting receipts of $15.4 billion for 280 MHz of C-Band spectrum).

[13] Press Release, *Clyburn, Pallone, and 10 House Dems Announce Plan to Connect All Americans to Affordable Broadband Internet*, Apr. 30, 2020, https://www.majoritywhip.gov/?press=clyburn-pallone-and-10-house-dems-announce-plan-to-connect-all-americans-to-affordable-broadband-internet.

B. Make Transformative Investments in Federal Spectrum Management to Encourage Efficiency and Greater Commercial Use.

The executive branch directly controls most of the nation's spectrum resources, and federal agencies therefore have an important obligation to manage spectrum well. Significant strides are still required to help increase the efficiency of federal use. At present, NTIA receives a relatively miniscule annual appropriation on the order of $40 million, even as its work is essential to making more spectrum available via auctions that often repay the government by the hundredfold. There are recent signs of progress as the Spectrum IT Modernization Act was recently marked up by the Senate Commerce Committee.[14] The bill has support from the chairs and ranking members of the Armed Services Committee, which is notable on an issue that has sparked jurisdictional and interagency disagreements far more than partisan ones.

Even so, the bill needs funding and the Administration should consider proposing more transformational investments to strengthen NTIA. At present, the agency lacks a permanently-confirmed Administrator with the ability and political standing to drive a holistic national spectrum policy – one that accounts for both defense and economic security priorities in a balanced way. The rise of 5G infrastructure security concerns to prominence has merely highlighted that good spectrum policy is essential to national economic security, so the time is right for Congress and the Administration to treat it as such by investing in federal spectrum management specifically at significantly higher levels.

Commercial spectrum. On the whole, the federal government has done an admirable job over the past decade making spectrum available for commercial wireless use. Congress authorized and the FCC conducted the first-ever voluntary incentive auction, making low-band

[14] S. 3717, 116th Cong. (marked up by Senate Commerce Committee on May 20, 2020), https://www.congress.gov/bill/116th-congress/senate-bill/3717/text.

spectrum in the 600 MHz band available.[15] The FCC took forward-looking action to make high-band spectrum in the 28 GHz band and other millimeter-wave bands available in the United States even before the World Radio Conference acted.[16] The agency is also enabling innovative spectrum-sharing techniques in the 3.5 GHz band and new public-private cost-recovery mechanisms in the C-Band, each making valuable mid-band spectrum available.[17] Meanwhile, the government has also taken important complementary steps to make unlicensed spectrum available for Wi-Fi and other technologies, including the FCC's planned opening of the 6 GHz band as well as some millimeter-wave bands.[18] Wi-Fi already carries the majority of mobile data traffic through offloading, and by 2023 approximately 75 percent of all networked devices in North America will either be wired or connected over Wi-Fi.[19]

---

[15] 2012 Spectrum Act § 6403; FCC, *Broadcast Incentive Auction and Post-Auction Transition*, https://www.fcc.gov/about-fcc/fcc-initiatives/incentive-auctions (visited June 24, 2020).

[16] Report and Order and Further Notice of Proposed Rulemaking, *Use of Spectrum Bands Above 24 GHz For Mobile Radio Services*, GN Docket No. 14-177, *et al.*, FCC 16-89 (rel. July 14, 2016) ("Spectrum Frontiers Report and Order").

[17] Report and Order, *Promoting Investment in the 3550-3700 MHz Band*, GN Docket No. 17-258, FCC 18-149 (rel. Oct. 24, 2018); Report and Order and Order of Proposed Modification, *Expanding Flexible Use of the 3.7 to 4.2 GHz Band*, GN Docket No. 18-122, FCC 20-22 (rel. Mar. 3, 2020).

[18] Report and Order and Further Notice of Proposed Rulemaking, *Unlicensed Use of the 6 GHz Band*, ET Docket No. 18-295, et al., FCC 20-51 (rel. Apr. 24, 2020).

[19] Press Release, *Cisco: Global Mobile Networks Will Support More Than 12 Billion Mobile Devices and IoT Connections by 2022; Mobile Traffic Approaching the Zettabyte Milestone*, Feb. 19, 2019, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1967403 ("In 2017, 54 percent of total mobile data traffic was offloaded; by 2022, 59 percent of total mobile data traffic will be offloaded."); Cisco, *Cisco Annual Internet Report (2018-2023)*, at 4, updated Mar. 9, 2020, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf ("By 2023, [North America] will have 25 percent of all networked devices mobile-connected and 75 percent will be wired or connected over Wi-Fi.").

All of these efforts reflect innovative thinking and leadership by U.S. policymakers. However, such efforts are not merely helpful, but are essential due to the historic legacy of U.S. spectrum allocations in earlier eras that makes re-allocation more difficult when compared to other countries with more greenfield bands available. Thus, this work must continue.

C. Create a "Research Dividend" to Invest in U.S. Research and Development in Wireless and Related Technologies.

5G, Wi-Fi 6, Bluetooth, and other leading wireless technologies have each resulted from substantial investment in research and development, and the United States must deepen its investment in wireless R&D to stay competitive. New technologies lead to new applications based on higher-bandwidth, lower-latency applications, and will also allow spectrum to be used more efficiently, making more effective use of a scarce national resource. As described above, *all* future spectrum auction revenues should be re-invested into the ICT sector, but in doing so a meaningful percentage – a **"research dividend"** – should be re-invested into R&D for new wireless technologies. Similar proposals have recently been made to invest a portion of auction revenues into broadband deployment – a so-called "rural dividend."[20] While laudable even as they should be more ambitious, those proposals must be paired with an R&D component.

The 2012 Spectrum Act provided some funding to NIST for wireless R&D specifically related to public safety communications research.[21] While Congress considered a broader program of more fundamental research, it was not ultimately included in the final law.[22] Meanwhile, many of the areas considered for funding in 2012 remain important needs today.

---

[20] *See, e.g.*, AIRWAVES Act § 5, S. 2223 (116th Cong.) (allocating 10 percent of auction proceeds to broadband deployment in underserved or unserved areas).

[21] 2012 Spectrum Act §§ 6413(b)(4), (b)(7).

[22] Public Safety Spectrum and Wireless Innovation Act § 224, S. 911, 112th Cong. (2012), https://www.congress.gov/bill/112th-congress/senate-bill/911/text.

Thus, after establishing a dedicated source of funding for wireless R&D (see above), research should be focused in the following areas, among others:

- opportunistic spectrum sharing;
- wireless cyberphysical systems;
- more efficient use of the wireless spectrum;
- dynamic spectrum access, including cognitive radio technologies;
- interference mitigation;
- emerging user interface and sensing technologies;
- wireless ad hoc networks;
- network resiliency and cybersecurity;
- communications interoperability, particularly between heterogeneous network technologies;
- pervasive information technology;
- nanoelectronics for communications applications;
- low-power communications electronics; and
- networking protocols and architectures.[23]

The rapid rise of global competition is forcing the United States to address the fact that it has been underinvesting in telecommunications research and development in recent decades. Taking steps to identify a dedicated funding source, and targeting it appropriately, will help ensure that the U.S. maintains its leadership in the coming decades.

D. Enact Legislation to Streamline Broadband Infrastructure Siting.

In the past two years, the Administration's American Broadband Initiative has taken helpful steps to streamline broadband infrastructure deployment on federal lands and leverage federal assets.[24] This has included some tangible accomplishments like the updating of a common application form in February 2020 for broadband providers to use across multiple

[23] *Id.*; *see also* Telecommunications Industry Association, *Spectrum Sharing Research and Development*, https://www.tiaonline.org/wp-content/uploads/2018/05/TIA_Spectrum_Sharing_Research_and_Development_White_Paper.pdf.

[24] *See, e.g.*, NTIA *et al.*, *American Broadband Initiative Milestones Report* (Feb. 2019), https://www.ntia.doc.gov/report/2019/american-broadband-initiative-milestones-report.

agencies.[25] In addition, the FCC has issued a series of orders that take common-sense steps to reduce obstacles to deployment posed by state and local regulations.[26] In many cases, those regulations were originally designed for large towers rather than the small cells that will play a larger role in 5G and future network deployments. However, the FCC's actions have been challenged in court with the agency's most significant streamlining order from September 2018 remaining under litigation.[27] This has created uncertainty and continues to delay 5G network deployments.

Congress has recently considered options to streamline wireless infrastructure deployment, but even bipartisan legislation has failed to advance.[28] Meanwhile, the COVID-19 pandemic has demonstrated once and for all that high-quality Internet access is essential to maintaining national and economic security, and indeed essential to every American citizen. The Administration and Congress should therefore reframe the need for effective broadband deployment as a national security issue – one no less important than other types of infrastructure. Federal legislation should be enacted to streamline broadband deployment, removing uncertainty and enabling more rapid access to next-generation technologies by every American.

---

[25] NTIA BroadbandUSA, *Federal Permitting: Overview*, https://broadbandusa.ntia.doc.gov/ntia-resources/federal-permitting-overview (visited June 17, 2020) (describing inclusion of telecommunications in the SF-299 Common Application Form).

[26] Orders in WT Docket No. 17-79, *Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment*, include the Report and Order, FCC 17-153 (rel. Nov. 17, 2017), the Second Report and Order, FCC 18-30 (rel. Mar. 30, 2018), and the Declaratory Ruling and Third Report and Order, FCC 18-133 (rel. Sept. 27, 2018), among other steps the agency has taken.

[27] *City of Eugene v. FCC*, 9th Cir., No. 19-70344 (oral arg. held Feb. 10, 2020) (reviewing the FCC's September 2018 order streamlining the state and local permitting process).

[28] *See, e.g.*, STREAMLINE Small Cell Deployment Act, S. 1699 (116th Cong.).

E. Promote Workforce Training for Broadband Deployment.

The United States faces a shortage of workers for broadband deployment. Estimates suggest that 20,000 job openings for tower climbers and telecommunications technicians must be filled in order to complete the country's 5G build.[29] The concern is not merely hypothetical; the FCC was forced to adopt a lengthy 39-month post-auction transition period for the 600 MHz band incentive auction in part because there were "a limited number of tower crews" qualified to do the necessary work.[30]

Meanwhile, the country is currently experiencing high unemployment due to COVID-19, which creates an opportunity to promote the necessary vocational training by building on existing efforts. For example, the FCC's Broadband Deployment Advisory Committee ("BDAC") has a working group focused on job skills and workforce training, and FCC Commissioner Brendan Carr has announced a 5G Jobs Initiative focused on community colleges.[31] In Congress, bipartisan bills have been introduced in both the House and Senate to draw greater attention to these issues, and the Senate Commerce Committee held a hearing on this topic in early 2020.[32] The Administration should support these and other efforts to ensure

---

[29] FCC, Broadband Deployment Advisory Committee, https://www.fcc.gov/broadband-deployment-advisory-committee (visited June 24, 2020); *see, e.g.*, Remarks of FCC Commissioner Brendan Carr, MWC-Barcelona, Feb. 25, 2019, at 4, https://docs.fcc.gov/public/attachments/DOC-356317A1.pdf.

[30] Report and Order, *Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, GN Docket No. 12-268, FCC 14-50, at ¶ 566 (rel. June 2, 2014).

[31] Press Release, *Carr Announces Initiative on Community Colleges as Pipelines for 5G Jobs*, Apr. 18, 2019, https://docs.fcc.gov/public/attachments/DOC-357096A1.pdf.

[32] Telecommunications Skilled Workforce Act, S. 3355 (116th Cong.) (introduced Feb. 27, 2020); TOWER Infrastructure Deployment Act, H.R. 3255 (116th Cong.) (introduced June 14, 2019); *The 5G Workforce and Obstacles to Broadband Deployment*, Hearing before the Senate Commerce Committee, Jan. 22, 2020, https://www.commerce.senate.gov/2020/1/the-5g-workforce-and-obstacles-to-broadband-deployment/a753f360-1f29-4450-9058-66f884b32905.

that worker shortages do not slow down 5G deployment at a moment when other countries are also pushing to deploy networks rapidly.

III. LINE OF EFFORT TWO: ASSESS RISKS TO AND IDENTIFY CORE SECURITY PRINCIPLES OF 5G INFRASTRUCTURE.

Security is foundational to the successful rollout of 5G infrastructure. Adoption of technologies that ride atop the 5G network, and achieving the myriad benefits such technologies can provide, will rely on trust built into connected infrastructure. This trust will be based on the ICT ecosystem's ability to manage and communicate risks across a variety of disparate stakeholders – public and private, large and small, domestic and international – and across nearly every sector of the economy.

While 5G technologies have been developing, stakeholders have identified several kinds of security challenges, chief among them: 1) how to foster a trusted and diverse base of telecommunications suppliers, and 2) how to effectively manage a broadening threat aperture with a new and increasing number of threat vectors as more of the physical world connects to wireless networks and more functionality, particularly critical functions, are virtualized. At the same time, the increased capacity, lower latency, and ability to tailor traffic across the 5G network offers new tools to more effectively manage risk.

As discussed below, the U.S. government has an opportunity to lead in addressing these challenges to shape an ecosystem based on a trusted foundation that can adapt as technology evolves and leverages the best of what the nation can offer. To do so will require an all-hands-on-deck, holistic approach across the public sector; doubling down on key partnership efforts to generate rules and policies, share information, and address emerging threats; leveraging leadership in the private sector to find and build technical solutions; and deeper collaboration with like-minded nations to shape common norms and values for next generation security.

A. Leverage the Technical Security Features Inherent in 5G Networks.

As a preliminary matter, government policy regarding 5G infrastructure security should both acknowledge and leverage the fact that 5G radio networks are more technically secure and robust than any prior generation. Security-by-design is incorporated into 5G architectural standards, and the new capacity achieved by 5G infrastructure will provide novel opportunities to secure traffic and manage risk across the network.

With the advent of 5G, operators will be able to transform parts of the network into a set of logical networks on top of a shared infrastructure, tailoring each logical network to serve a defined function. Not only will this "network slicing" enable more efficient management of traffic, particularly as more of the physical world connects, but it will also enable operators to provide enhanced and tailored security features for more sensitive traffic, leveraging innovations in enhanced encryption, machine learning, and other emerging technologies. This strong technical foundation should inform and factor into the risk-based approach to 5G security discussed below.

B. Rely on Whole-of-Government, Risk-Based Approaches to Address 5G Security Challenges.

Other countries are pursuing integrated economic security strategies to favor "national champion" companies in the global telecommunications marketplace. To stay competitive, the United States must rely on a whole-of-government strategy and coordination to leverage all the tools at its disposal in support of a rules-based, competitive market that offers a variety of trusted suppliers with high-quality products. To help trusted suppliers address evolving 5G security challenges most effectively, the U.S. government should pursue risk-based approaches to security and empower other organizations to do the same.

To that end, consistent with the recommendations of the Cyberspace Solarium Commission ("CSC") Report, the Implementation Plan should include steps to **bolster the Cybersecurity and Infrastructure Security Agency ("CISA")** as lead agency for federal cybersecurity.[33] The government should leverage CISA's expertise and working relationship with key critical infrastructure stakeholders to identify and manage strategic risks related to 5G. Additionally, the Administration should adopt the CSC Report's recommendation to **establish a National Cyber Director** to serve as the President's principal advisor for cybersecurity issues related to 5G.[34] The National Cyber Director should lead national-level coordination for 5G cyber strategy, policy, and defensive cyber operations.

In managing threats posed by untrusted suppliers to federal 5G networks, the government should **rely on the Federal Acquisition Security Council ("FASC") process** established by the 2018 SECURE Technology Act.[35] The FASC serves as the key mechanism for the federal government to aggregate information and communications technology and services ("ICTS") threat information, make recommendations regarding federal supply chain risk management ("SCRM") standards and best practices, develop certain information sharing criteria, and recommend exclusion or removal orders of covered ICTS from untrusted sources from the

---

[33] *See* Cyberspace Solarium Commission Report, Mar. 2020, at 39, Key Recommendation 1.4, https://www.solarium.gov ("Congress should strengthen the Cybersecurity and Infrastructure Security Agency (CISA) in its mission to ensure national resilience of critical infrastructure, to promote a more secure cyber ecosystem, and to serve as the central civilian cybersecurity authority to support federal, state and local, and private-sector cybersecurity efforts. Congress should strengthen the Cybersecurity and Infrastructure Security Agency (CISA) in its mission to ensure national resilience of critical infrastructure, to promote a more secure cyber ecosystem, and to serve as the central civilian cybersecurity authority to support federal, state and local, and private-sector cybersecurity efforts.")

[34] *See id.* at 37, Key Recommendation 1.3.

[35] Pub. L. No. 115-390, 132 Stat. 5173 (2018).

federal supply chain. While the government may find it necessary to exclude certain untrusted suppliers from domestic networks, it should do so through mechanisms like the FASC, which are narrowly tailored, transparent, and afford due process. It should **avoid ad hoc actions** that run the risk of creating inconsistency across federal agencies and unnecessarily harm the broader ICTS ecosystem.

C. Support Public-Private Partnership Efforts to Develop Risk Management Tools and Guidance.

Given that the vast majority of 5G infrastructure will continue to be owned and operated by the private sector and no single entity has visibility and control over the network as a whole, partnership continues to be critical in identifying and managing risks to communications networks. Partnerships between the public and private sector and across agencies enable solutions that leverage the insight and expertise of the diversity of 5G network stakeholders, and favor solutions that can be tailored to meet individual needs and remain durable over time.

To foster more effective risk management across the broad 5G ecosystem, the Implementation Plan should include **support** for key public-private partnership efforts, such as the **Department of Homeland Security ICT Supply Chain Risk Management Task Force,** which serves as the preeminent convening body for SCRM collaboration between the federal government, IT, and Communications Sectors.[36] Other key efforts such as the National Security Telecommunications Advisory Committee **("NSTAC")** and the Federal Communications Commission's Communications Security Reliability and Interoperability Council **("CSRIC")**

[36] Dep't. of Homeland Security, *Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force*, (last revised June 15, 2020), https://www.cisa.gov/ict-scrm-task-force

have and will continue to provide important guidance on emerging challenges facing communications security.

The Implementation Plan should also include discussion regarding how agencies and the private sector can **leverage NIST guidance** to support risk-management across the 5G network and among the technologies with which it will connect. For example, the NIST Framework for Improving Critical Infrastructure Cybersecurity has emerged as a key tool in identifying, managing, and communicating cybersecurity risks across sectors and internationally.[37] With the convergence of sectors looking to next-generation wireless networks as core to their functionality, tools like the NIST Cybersecurity Framework and the suite of NIST guidance that addresses more specific aspects of the network will be crucial to managing and communicating risks across the diverse 5G ecosystem.

D. Support Established International Standards Organizations to Develop Technical Guidance.

In building out new 5G architecture and evolving the network toward future generations, international standards organizations remain a vital forum for developing common solutions to technical challenges. The Implementation Plan should **recognize and support ongoing efforts at 3GPP and elsewhere** in developing the architectural standards that define 5G and its future iterations, including key security requirements that will provide new opportunities to more effectively manage risks.[38] These standards will help enable 5G network providers to create secure network slices for customers with enhanced encryption protecting traffic across the network, and more.

---

[37] Nat'l Inst. of Standards and Technology ("NIST"), *Cybersecurity Framework*, updated May 21, 2020, https://www.nist.gov/cyberframework/framework.

[38] *See e.g.*, 3GPP, *About 3GPP*, https://www.3gpp.org/about-3gpp (visited June 24, 2020).

That said, not all standards organizations operate in the same way and each organization is not equally appropriate to address all security challenges. For example, the ITU-T, which operates based on a country-by-country vote, is not an appropriate venue to develop fundamental changes to the Internet Protocol or address 5G supply chain security.[39] While it is essential to support the integrity and ability of international standards organizations to develop technical solutions to challenges facing the 5G ecosystem, the Administration should be careful to avoid actions that could politicize the standards process. Efforts by other countries to unduly influence the outcome of international standards should be met with strong censure by the international community and the U.S. should **lead the way in promoting a rules-based, industry-driven marketplace** for 5G technologies.

E. Collaborate with Like-Minded Nations on Values, Norms, and Rules of the Road.

In order to inculcate an international culture of secure and trusted communications networks, the United States must build a strong coalition of like-minded allies and partners willing to collectively leverage their power to enforce norms of responsible behavior. The State Department has already made significant strides in developing and promoting the Prague Proposals in partnership with the Czech Republic and entering into memoranda of understanding ("MOUs") with other nations in support of the Proposals.[40] The Implementation Plan should include meaningful steps to provide additional support for the State Department's efforts to

[39] *See* CompTIA Comments to NTIA, "Input on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly," (June 8, 2020), https://www.ntia.doc.gov/federal-register-notice/2020/comments-proposals-positions-wtsa20.

[40] Gov't of the Czech Republic, *The Prague Proposals*, May 3, 2019, https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

promote the Proposals, enter additional MOUs, and make good on the Proposals in partnership with other agencies and organizations. (*See also* section V below.)

IV. LINE OF EFFORT THREE: ADDRESS RISKS TO U.S. ECONOMIC AND NATIONAL SECURITY DURING DEVELOPMENT AND DEPLOYMENT OF 5G INFRASTRUCTURE WORLDWIDE.

Addressing the economic and national security risks associated with 5G infrastructure deployment will be a continuing issue for the government in the years ahead, not least because 5G deployments are already underway throughout the world. Line of Effort Three recognizes this, but the National Strategy identifies just two specific objectives: (1) to manage the supply chain risks in U.S. government infrastructure, including 5G; and (2) to address the risk of 'high-risk' vendors in U.S 5G infrastructure.[41] Efforts to address them are well underway, including several laws enacted by Congress, the President's Executive Order on Securing the Information and Communications Technology and Services Supply Chain ("EO 13873"), and the FCC's open proceeding on Protecting Against National Security Threats to the Communications Supply Chain.[42] In some cases, refinements are needed: the first draft rule implementing EO 13873, as well as section 889(a)(1)(B) of the FY19 National Defense Authorization Act ("Part B"), each created significant scoping problems that have not yet been addressed.[43]

---

[41] National Strategy to Secure 5G at 4-5.

[42] Exec. Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, May 15, 2019, 84 Fed. Reg. 22689 (May 17, 2019); FCC WC Docket No. 18-89, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*; Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124 (Mar. 12, 2020).

[43] *See* Comments of CompTIA, filed Jan. 10, 2020 in Docket No. DOC-2019-0005, *Securing the Information and Communications Technology and Services Supply Chain* (discussing scoping problems with the EO 13873 draft rule); CompTIA Presentation to OMB on Section 889(a)(1)(B), Mar. 31, 2020, https://www.reginfo.gov/public/do/eoDownloadDocument?pubId=&eodoc=true&documentID=6166; Jenny Leonard and Shelly Banjo, *A Quiet Panic Is Growing in U.S. Boardrooms Over*

The RFC sensibly goes further by asking not just about risks, but also about the opportunities that deployment of 5G networks worldwide create for U.S. companies.[44] Indeed, the opportunity for U.S. leadership is significant, not just in 5G but future generations of wireless technology. The RFC also correctly asks about promoting 5G vendor diversity and fostering market competition. This implies the correct approach, as the government should focus on pro-competitive measures while avoiding heavy-handed intervention into the marketplace.

A. Encourage Market Trends Toward Open Architectures and Virtualization.

The emerging 5G landscape offers significant promise, not least because of market trends toward open architectures and virtualization in radio access network ("RAN") technology. For example, Open RAN is an architectural approach that seeks to disaggregate RAN functionality by using open interface specifications.[45] The O-RAN Alliance, among other groups, is working toward specifying application programming interfaces ("APIs") and other interfaces for such open architectures.[46] Meanwhile, virtualized RAN ("vRAN") implements RAN functions by placing them in specialized software that can run on commodity hardware based on general-purpose processors.[47] Both Open RAN architectures and vRAN implementations are poised to

---

Huawei Ban, BLOOMBERG, June 10, 2020, https://www.bloomberg.com/news/articles/2020-06-10/dread-over-impending-anti-huawei-law-grows-at-u-s-companies.

[44] RFC, 85 Fed. Reg. at 32017 ("Line of Effort Three … (1) What opportunities does the deployment of 5G networks worldwide create for U.S. companies?").

[45] *See, e.g.*, Michelle Shelton, Parallel Wireless, *Open RAN Terminology – Understanding the Difference Between Open RAN, OpenRAN, ORAN, and More*, Apr. 20, 2020, https://www.parallelwireless.com/open-ran-terminology-understanding-the-difference-between-open-ran-openran-oran-and-more/; John Baker, Mavenir, *What is the Difference Between OpenRAN, O-RAN and vRAN?*, Mar. 20, 2020, https://mavenir.com/blog/what-is-the-difference-between-openran-o-ran-and-vran/.

[46] *See* O-RAN Alliance, *O-RAN: Towards and Open and Smart RAN*, Oct. 2018, *available at* https://www.o-ran.org/specifications.

[47] *See, e.g.*, Wind (an Intel Company), *vRAN: The Next Step in Network Transformation*, https://builders.intel.com/docs/networkbuilders/vran-the-next-step-in-network-

significantly transform the wireless ecosystem, not least because they will lower barriers to entry and promote greater competition.

To be clear, CompTIA supports technology neutrality and the federal government should not pick specific winners and losers in the marketplace. Indeed, aside from different 5G implementations, other technologies such as Wi-Fi 6 may be appropriate for some use cases. That said, the rise of open architectures for RAN infrastructure and/or virtualized networking products are both trends that favor the United States. First, by lowering barriers to entry, open architectures will favor countries that already possess a strong technology development ecosystem, including startups, established players, and well-capitalized companies in related fields who are considering entering the market. Second, virtualization will generally promote U.S. economic and national security interests because the nation remains a global leader in software development, even as other countries have claimed a greater share of hardware manufacturing.

The federal government should therefore consider ways to encourage these trends without dictating outcomes. For example, federal agencies could use their purchasing power to buy systems that are considered to be standards-based or that offer stronger features regarding upgradeability and interoperability. Open architectures and virtualized implementations are not the only way to achieve high performance on such metrics, but they would likely score well. The government could also support research, development, and standardization efforts

---

transformation.pdf; Samsung, *Transition to Virtualized RAN*, https://www.samsung.com/global/business/networks/products/radio-access/virtualized-ran/ (visited June 24, 2020) ("Samsung's vRAN liberates operators from static, hardware-bound network operations, and enables versatile, software-centric operations.").

specifically targeted toward virtualization and open architectures; such efforts have heretofore been largely undertaken by the private sector alone.

B. Invest in the Ecosystem, Not Specific Companies.

The best way to "promote 5G vendor diversity and foster market competition," as the RFC asks, is to promote the technology ecosystem as described above.[48] Along with promoting technology neutrality, the government should not favor particular business models or even specific vendors. For example, some have suggested that the U.S. government should purchase an equity stake in certain wireless equipment manufacturers.[49] These proposals should be ruled out.

First, as explained above, the market is changing rapidly enough that direct federal intervention of this nature would be myopic and likely a bad investment for American taxpayers. Second, such direct intervention would likely harm innovation. Third, the solution to the problem of other countries like China providing massive subsidies to "national champion" companies like Huawei is surely not for the United States to *emulate* China. Rather, the solution is to leverage and double-down on U.S. strengths, including investing in research and development and a skilled labor force, and fostering a business climate that encourages experimentation and rewards the best new ideas.

---

[48] RFC, 85 Fed. Reg. at 32017 ("Line of Effort Three … (3) How should the U.S. Government best promote 5G vendor diversity and foster market competition?").

[49] Attorney General William Barr, *Attorney General William P. Barr Delivers the Keynote Address at the Department of Justice's China Initiative Conference*, Remarks as Prepared for Delivery, Feb. 6, 2020, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-department-justices-china ("Some propose that these concerns could be met by the United States aligning itself with Nokia and/or Ericsson through American ownership of a controlling stake, either directly or through a consortium of private American and allied companies. Putting our large market and financial muscle behind one or both of these firms would make it a more formidable competitor and eliminate concerns over its staying power. We and our closest allies certainly need to be actively considering this approach.").

V. LINE OF EFFORT FOUR: PROMOTE RESPONSIBLE GLOBAL DEVELOPMENT AND DEPLOYMENT OF 5G.

As noted above, collaboration between like-minded nations in support of common values in next-generation telecommunications is fundamental to protecting the security, privacy, and prosperity of communications technology users. To that end, the State Department has already made meaningful strides in promoting responsible global development and deployment of 5G, including its work to develop and advance the Prague Proposals in partnership with the Czech Republic.[50] That said, in order to support global development of secure and trusted communications technologies, the government needs more positive incentive tools. As described below, there are a variety of specific steps the Administration and Congress can take to provide them.

A. Establish the Multilateral Telecom Security Fund.

As envisioned in the USA Telecommunications Act introduced earlier this year, the Multilateral Telecom Security Fund would be made available to support work with foreign partners to accelerate the adoption of trusted and secure equipment globally and to encourage multilateral participation.[51] This fund would provide the State Department with necessary resources to support collaboration with like-minded nations in support of trusted international 5G and future generation infrastructure. The concept for this fund has since been included in the

[50] Government of the Czech Republic, *The Prague Proposals*, May 3, 2019, https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

[51] S. 3189 § 2(c)(2), 116th Cong. ("The Secretary of State, in consultation with the NTIA Administrator, the Secretary of Homeland Security, the Secretary of the Treasury, the Director of National Intelligence, and the [Federal Communications] Commission, shall establish a common funding mechanism, in coordination with foreign partners, that uses amounts from the Multilateral Telecommunications Security Fund to support the development and adoption of secure and trusted telecommunications technologies.").

proposed Intelligence Authorization Act for FY 2021 at a level of $750 million over 10 years, and the Administration should support this proposal.[52]

B. Revise the U.S. International Development Finance Corporation Rules to Support Strategic Telecom Investments.

The federal government should revise the U.S. International Development Finance Corporation ("DFC") rules to support deployment of trusted technologies in strategic locations that may be considered more developed but economically may not be equally able to choose trusted 5G suppliers. The European Energy Security and Diversification Act of 2019 eased the DFC's less-developed country requirement for energy infrastructure projects in Europe and Eurasia.[53] 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.

C. Revise the U.S. Export-Import Bank Rules to Support Trusted Telecom Suppliers.

As trusted suppliers compete in the global marketplace with suppliers of concern that benefit from sweetheart financing terms from state-owned banks, the U.S. should leverage the EXIM Bank to support trusted suppliers.[54] To do so, the EXIM Bank's content rules dating from the 1970s and 1980s must be revised to reflect contemporary value chains. The current rules require products to contain 85% U.S. content to be eligible for full EXIM financing, which is an

---

[52] Intelligence Authorization Act for Fiscal Year 2021 §§ 501(b)(2), (b)(3)(B), S. 3905, 116th Cong. (as introduced on June 8, 2020).

[53] Pub. L. No. 116-94, Div. P, Title XX, § 2004(e)(1)(A), 133 Stat. 2534, 3225 (Dec. 20, 2019).

[54] *See, e.g.*, Chuin-Wei Yap, *State Support Helped Fuel Huawei's Global Rise*, WALL ST. J., Dec. 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736 (finding that Huawei had access to as much as $75 billion in state support).

extremely difficult threshold for most of the telecom equipment industry to meet.[55] Where in the 1970s and 1980s U.S. widgets were the primary export, most U.S. technology companies now develop products domestically but manufacture/assemble their products at least partially abroad. Meanwhile, the United States continues to be one of the world's wealthiest nations in part because of its sustained focus on intellectual property development. The EXIM Bank must therefore revise its rules to reflect this reality and partner with industry in support of collective 5G security goals.

Not only is such a revision necessary to support national security, but it is also statutorily required to support the new "Program on China and Transformational Exports" established in the EXIM Bank's 2019 reauthorization.[56] To support this revision, the EXIM Board can waive the content threshold entirely, but that is an arduous process and would be applied ad hoc rather than effectively revising the rules for the technology industry overall. Instead, the EXIM Bank should adopt a more flexible approach to U.S. content rules that takes into account the percentage of U.S.-based R&D and IP and significantly lowers the U.S. content requirements to support the national security imperative to finance deployment of secure and trusted telecommunications infrastructure.

---

[55] EXIM Bank, *Medium- and Long-Term Content Policy*, https://www.exim.gov/policies/content/medium-and-long-term (visited June 24, 2020) ("The total level of support for a[n] export contract will be the lesser of: 85% of the value of all eligible goods and services in the U.S. export contract; or 100% of the U.S. content in all eligible goods and services in the U.S. export contract"); *see also* Congressional Research Service, *Export-Import Bank: Overview and Reauthorization Issues*, at 8-9, updated Aug. 9, 2019, available at https://fas.org/sgp/crs/misc/R43581.pdf ("If the foreign content exceeds 15%, the Bank's support is lowered proportionally.").

[56] *See* EXIM Bank, *Fact Sheet, Overview: Program on China and Transformational Exports*, https://www.exim.gov/who-we-serve/external-engagement/china-and-transformational-exports-program/fact-sheet (visited June 24, 2020).

D. Promote U.S. Participation in Standards Development by Expanding the R&D Tax Credit While Avoiding Politicization of Technical Issues.

The U.S. approach to global standards, at least in the wireless space, has primarily been to have companies participate in those bodies rather than the government itself, while other countries such as China and Russia are represented more directly by their governments. In general, the U.S. approach continues to make sense. Unlike other countries which may have a few "national champions" in certain areas, or even just one company, the U.S. communications technology ecosystem is robustly competitive. Under these circumstances, identifying an "American position" on a technical issue either before or during a global standards meeting could be a difficult task. In addition to technically-driven proposals, some U.S. companies may also push for the inclusion of their intellectual property in a standard – that is, a standards-essential patent ("SEP") – while other companies may push for more open standards.

These are not matters for the federal government to adjudicate in technical standards bodies like 3GPP. However, the Department of Defense recently established a "tiger team" with the apparent goal of engaging global wireless standards bodies more directly.[57] While the implications of this have not been fully determined, such direct engagement by a federal agency – and specifically by a *security* agency – in global technical bodies creates the risk of politicizing the process. It also creates a potential risk of some U.S. companies being forced to work at cross purposes with their own government on important technical issues. DOD and other agencies should therefore carefully consider (or re-consider) the scope of any such involvement, with the primary goal of receiving and sharing information with U.S. industry that will benefit both the

[57] Justin Doubleday, *Pentagon Looks to Participate in 5G Standards-Setting Bodies*, Inside Defense, June 5, 2020, https://insidedefense.com/daily-news/pentagon-looks-participate-5g-standards-setting-bodies (subscription required).

public and private sector. That said, the United States should continue to advance the nation's interests in international bodies with country-based voting like the ITU, particularly when other countries make proposals that would harm U.S. or international interests.[58]

R&D tax credit for standards. A lack of government participation need not and should not equate to a lack of government support. The Administration should work with Congress to expand the R&D tax credit to encompass participation in global standards development activities. The standards process is closely related conceptually to research and development, often involving the same individuals within a company. Expansion of the credit would therefore likely have a more immediate policy effect, and would send a meaningful signal encouraging greater participation by the private sector. Even as U.S. industry has consistently opposed protectionist and other industrial policies implemented abroad, government investment in research and development is a legitimate, internationally-accepted method for countries to advance their technological leadership and economic competitiveness. Expanding the R&D tax credit to include standards development would also help the United States capitalize on greater federal investment into wireless R&D as described in section II-C above.

CONCLUSION

CompTIA supported the Secure 5G and Beyond Act of 2020 and we appreciate the opportunity to comment on the Implementation Plan. The Administration is right to consider a holistic approach to national and economic security issues related to 5G, although specific policies should consider emerging trends in wireless technologies and look to future generations as well. By reinvesting in network deployment and technology development, using risk-based

[58] *See* Comments of the Computing Technology Industry Association (CompTIA), filed June 8, 2020 in Docket No. 200521-0144 (opposing a potential "New IP" proposal from China that may be offered at the 2020 World Telecommunication Standardization Assembly later this year).

approaches to security that are built on partnerships, recognizing opportunities for U.S. companies in the future, and advancing U.S. interests globally, the United States can not only promote national and economic security but ensure that the nation is the global leader in both 5G and the technologies that will follow.

We appreciate the Administration's continued work on these important issues and look forward to continued engagement with the government as the Implementation Plan is developed and the National Strategy is put into place.

Sincerely,

/s/ Dileep Srihari

Dileep Srihari
Vice President and Senior Policy Counsel

Savannah Schaefer
Senior Director, Public Advocacy

COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION (CompTIA)
322 4th Street NE
Washington, DC 20002

June 25, 2020